Gängige Szenarien der Administration von ViPNet VPN

Anhang zum Benutzerhandbuch

infotecs

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Copyright

1991–2015 Infotecs GmbH, Berlin

Version: 00121-04 90 03 DEU

Dieses Dokument ist Teil des Softwarepaketes und unterliegt daher denselben Lizenzbestimmungen wie das Softwareprodukt.

Dieses Dokument oder Teile davon dürfen nicht ohne die vorherige schriftliche Zustimmung der Infotecs GmbH verändert, kopiert, weitergegeben etc. werden.

ViPNet ist ein registriertes Warenzeichen des Softwareherstellers Infotecs GmbH.

Marken

Alle genannten Markennamen sind Eigentum der jeweiligen Hersteller.

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhalt

Einführung **5**
Über dieses Dokument 6
Zielgruppe 6
Verwendete Konventionen 6
Kontakt 8
FAQ und andere Hilfsinformation 8
Kontakt 8

Kapitel 1. Das Programm ViPNet Network Manager auf einen anderen Computer übertragen **9**

Kapitel 2. Installation eines Remotedruckers im ViPNet Netzwerk **12**
Problemstellung formulieren 13
Drucker einrichten 14

Kapitel 3. Tunnelung von Knoten, die sich nicht im Subnetz des tunnelnden Coordinators befinden **16**

Kapitel 4. Besonderheiten einer integrierten Firewall **20**
Allgemeine Informationen 21
Einsatz der integrierten Firewall 22
Konfiguration der Netzwerkfilter zum Durchlassen des Traffics 23
Konfiguration der Netzwerkfilter für Clients 25
Konfiguration der Netzwerkfilter für Coordinatoren 29

Kapitel 5. Beispiel für die Verwaltung von Netzwerkknoten-Sicherheitsrichtlinien mit Hilfe von ViPNet Policy Manager **31**

Kapitel 6. Remote-Steuerung von ViPNet Netzwerkknoten **35**
Automatische Anmeldung in Windows und ViPNet Software 36
Wofür wird die automatische Anmeldung benötigt 36
Konfiguration der automatischen Anmeldung in Windows 36
Automatische Anmeldung in ViPNet Software einstellen 39
Konfiguration des Terminalservers bei Remotesteuerung 41
Installation der Software für Remotesteuerung 43
Starten des Programms für die Remotesteuerung 44

Kapitel 7. Verbindungen zwischen ViPNet VPN- Netzwerk und einem Netzwerk auf Basis der Software ViPNet Administrator 46

Allgemeine Informationen 47

Initiierung der Verbindung mit Hilfe des ViPNet Network Manager 48

Initiierung der Verbindung mit Hilfe der Software ViPNet Administrator 50

Anforderungen an die Partnernetzwerk-Informationen des ViPNet Netzwerks unter der Steuerung von ViPNet Administrator 52

Anhang A. Index 55

Einführung

Über dieses Dokument 6

Kontakt 8

Über dieses Dokument

Der vorliegende Anhang zum Handbuch „ViPNet VPN. Benutzerhandbuch“ enthält Beschreibungen von Szenarien, die darauf ausgerichtet sind, die bei der Administration des ViPNet VPN-Netzwerks häufig auftretenden Aufgaben zu lösen.

Zielgruppe

Dieses Dokument richtet sich an Administratoren, in deren Zuständigkeitsbereich die Konfiguration und Wartung des virtuellen privaten Netzwerks ViPNet VPN fällt.

Von den Lesern dieses Dokuments wird kein detailliertes Wissen im Bereich der Informationstechnologie verlangt. Eine erste allgemeine Vorstellung über Computernetzwerke, IP-Protokolle, Firewalls, Tunnelung und Kryptographie ist jedoch wünschenswert.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	Achtung! Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	Hinweis. Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.

Notation	Beschreibung
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Mitarbeitern der Firma „InfoTeCS GmbH“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.de.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 22 (Tel.); +49 (0) 30 206 43 66 66 (Fax).

1

Das Programm ViPNet Network Manager auf einen anderen Computer übertragen

Wenn in einem funktionierenden ViPNet VPN-Netzwerk das Programm ViPNet Network Manager auf einem anderen Computer installiert werden soll (zum Beispiel, weil der alte Computer gegen einen neuen ausgetauscht wird), sollten die existierende Netzwerkstruktur und die Programmeinstellungen von ViPNet Network Manager beibehalten werden.

Wenn die aktuelle Programmversion von ViPNet Network Manager aktualisiert werden soll, dann sollte das Upgrade unbedingt noch vor der Übertragung des Manager-Arbeitsplatzes auf den neuen Computer durchgeführt werden.

Es wird angenommen, dass bei der Übertragung des Managers auf einen neuen Computer folgende Bedingungen erfüllt sind:

- Der alte Computer ist funktionsfähig und das Programm ViPNet Network Manager läuft störungsfrei (Datenbank und Schlüsseldaten sind nicht beschädigt).
- Das Administratorpasswort von ViPNet Network Manager ist bekannt.
- ViPNet Network Manager wird entweder auf einen neuen Computer, auf welchem noch keine ViPNet Software installiert ist, oder auf einen funktionierenden ViPNet Client, der zum gegebenen Zeitpunkt nicht als Manager-Arbeitsplatz eingesetzt wird, übertragen.

Führen Sie die folgenden Schritte durch, um den Manager-Arbeitsplatz auf einen anderen Computer zu übertragen:

1. Wenn das Programm ViPNet Network Manager aktualisiert werden soll, dann führen Sie das Update auf dem alten Computer noch vor dem Übertragen des Manager-Arbeitsplatzes durch. Installieren Sie dazu die neue Version von ViPNet Network Manager, ohne dabei die alte Version des Programms zu deinstallieren.
2. Exportieren Sie auf dem alten Computer im Programm ViPNet Network Manager die ViPNet Programm- und Netzwerkparameter auf einen abnehmbaren Datenträger. Dazu:
   - Wählen Sie im Menü **Extras** den Eintrag **Konfiguration exportieren**.
   - Speichern Sie die Exportdatei der Konfiguration auf einem abnehmbaren Datenträger.
3. Installieren Sie ViPNet Network Manager auf dem neuen Computer. Es werden dabei automatisch das DBMS MS SQL Server 2008 R2 installiert und eine neue Datenbank angelegt.
4. Importieren Sie die ViPNet Network Manager-Konfiguration auf dem neuen Computer. Dazu:
   - Wählen Sie auf dem neuen Computer im Programm ViPNet Network Manager im Menü **Extras** den Befehl **Konfiguration importieren**.
   - Wählen Sie die Exportdatei der Konfiguration, die auf dem alten Computer erstellt wurde, und folgen den Anweisungen des Assistenten.

   Auf diese Weise werden die Struktur des ViPNet Netzwerks, die Netzwerknummer sowie die Lizenz- und Registrierungsdaten des Programms wiederhergestellt.
5. Registrieren Sie ViPNet Network Manager auf dem neuen Computer. Da der Code des neuen Computers vom Code des alten Computers abweicht, sollte eine Anfrage für einen neuen Registrierungscode erstellt und abgesendet werden.
6. Installieren Sie das Programm ViPNet Client oder ViPNet Coordinator auf dem neuen Computer (abhängig von dem Computer, der als Manager-Arbeitsplatz definiert wurde) und erstellen eine neue Schlüsseldistribution. Dazu führen Sie folgende Aktionen aus:
   - Wenn nötig, ändern Sie im Programm ViPNet Network Manager die Einstellungen (IP-Adresse, Firewall-Einstellungen und andere) des Netzwerkknotens, der als Manager-Arbeitsplatz auftritt.
   - Erstellen Sie eine Schlüsseldistribution (Datei DST) für den Administrator-Arbeitsplatz.
   - Stellen Sie sicher, dass der Netzwerkknoten, der auf dem alten Computer installiert war, nicht an das ViPNet Netzwerk angeschlossen ist.

Achtung! Im ViPNet Netzwerk dürfen keine zwei Netzwerkknoten mit der gleichen Schlüsselinformation existieren.

   - Installieren Sie auf dem neuen Computer die Software ViPNet Client und starten den Computer neu.
   - Installieren Sie die erstellte Schlüsseldistribution (Datei DST) für den neuen Manager-Arbeitsplatz.

7. Wenn das Programm ViPNet Client bereits auf dem Computer installiert ist, führen Sie folgende Aktionen aus:
    - Wählen Sie in der Navigationsleiste von ViPNet Network Manager den Netzwerkknoten, der als Manager-Arbeitsplatz auftreten soll.
    - Klicken Sie mit der rechten Maustaste auf dem Netzwerkknoten und wählen im Kontextmenü **Als Manager-Arbeitsplatz festlegen**.
    - Erstellen Sie eine neue Schlüsseldistribution für den neuen Manager-Arbeitsplatz und auch für den Netzwerkknoten, der vorher ein Manager-Arbeitsplatz war.
    - Installieren Sie die erstellte Schlüsseldistribution (Datei DST) für den neuen Manager-Arbeitsplatz auf dem neuen Computer.
    - Entfernen Sie das Programm ViPNet Network Manager auf dem alten Computer und installieren die erstellte Schlüsseldistribution für den entsprechenden Netzwerkknoten.
8. Das Programm ViPNet Network Manager auf dem neuen Computer ist nun einsatzbereit.

Ausführliche Informationen finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch“:

- über die Installation des Programms ViPNet Network Manager, ViPNet Client und ViPNet Coordinator – Kapitel 2 „Installation und Deinstallation von ViPNet VPN“,
- über die Registrierung des Programms ViPNet Network Manager – Kapitel 17 „Registrierung von ViPNet Network Manager“,
- über die Installation der Schlüsseldistribution – Kapitel 5 „Verwaltung des ViPNet Netzwerkes“, Abschnitte „Speichern der Schlüsseldistributionen“ und „Versand und Speicherung der Netzwerkknotenschlüssel“.

2

Installation eines Remotedruckers im ViPNet Netzwerk

Problemstellung formulieren 13

Drucker einrichten 14

Problemstellung formulieren

Nehmen wir an, es gibt im Büro einen gemeinsamen Drucker, der an einen der ViPNet Netzwerkknoten (Computer A) angeschlossen ist. Die Benutzer anderer ViPNet Netzwerkknoten (sowohl stationärer als auch mobiler) möchten auf diesen Drucker zugreifen. Dabei verfügen die Computer im Büro über dynamische IP-Adressen, die sich ändern können.

Abbildung 1. Remotedrucker verwenden

Betrachten wir die Reihenfolge der Schritte bei der Installation eines Netzwerkdruckers auf Computer B, falls folgende Bedingungen eingehalten werden:

- Computer A befindet sich im Punkt A.
- Computer B befindet sich im Punkt B.
- An Computer A ist ein Drucker angeschlossen, der im Betriebssystem des Computers A installiert und für den öffentlichen Zugang freigegeben ist.
- Sowohl auf Computer A als auch auf Computer B ist ViPNet Software installiert.
- Computer A und Computer B können innerhalb des ViPNet Netzwerks aufeinander zugreifen.
- Die Art der Verbindung zum Internet spielt bei Computer A und Computer B keine Rolle.

Vom Computer B soll ein Dokument zum Drucker, der an Computer A angeschlossen ist, zum Drucken gesendet werden.

Damit ein Dokument vom Computer B an den Drucker weitergeleitet werden kann, sollte zunächst dieser Drucker auf Computer B als Netzwerkdrucker eingerichtet werden.

Drucker einrichten

Führen Sie auf Computer B die folgenden Schritte aus, um das Drucken von Dokumenten vom Computer B aus zu ermöglichen (auf Computer A sind keine weiteren Einstellungen erforderlich):

1 Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Befehl **Anwendungseinstellungen**.

Hinweis. Wenn Sie das Programm ViPNet Client Monitor verwenden, dann sollten Sie alle Einstellungen im Administratormodus durchführen.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Allgemeine** und aktivieren anschließend im Panel-Ansicht das Kontrollkästchen **IP-Adressen im Ordner „Privates Netzwerk" anzeigen**.

3 Klicken Sie auf **OK**.

Im Bereich **Privates Netzwerk** werden nun die sichtbaren IP-Adressen aller Knoten des aktuellen ViPNet Netzwerks abgebildet.

4 Doppelklicken Sie im Bereich **Privates Netzwerk** auf Computer A.

Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.

5 Wechseln Sie im Fenster **Netzwerkknoten-Eigenschaften** zur Registerkarte IP-Adresse und stellen sicher, dass dort das Kontrollkästchen **Virtuelle IP-Adresse verwenden** aktiviert ist. Falls das Kontrollkästchen nicht verfügbar ist, wenden Sie sich an den Administrator Ihres ViPNet Netzwerks oder an den technischen Kundendienst der Firma „Infotecs". Merken Sie sich die virtuelle IP-Adresse, die in der Registerkarte **IP-Adresse** abgebildet ist (wenn mehrere IP-Adressen aufgeführt sind, merken Sie sich nur die erste). Standardmäßig haben virtuelle Adressen die Form 11.*.*.*, zum Beispiel 11.0.0.15.

6 Wechseln Sie zur Registerkarte **Allgemeine** und merken sich den Namen von Computer A. Schließen Sie danach das Fenster **Netzwerkknoten-Eigenschaften**.

7 Öffnen Sie die Datei `%systemroot%\system32\drivers\etc\hosts` zum Bearbeiten und fügen dort die folgende Zeile ein:

```
<Virtuelle IP-Adresse Computer A><Leerzeichen><Name Computer A>
```

Zum Beispiel: `11.0.0.15 pc15`

8 Stellen Sie sicher, dass der Name des Computers richtig umgewandelt wird, indem Sie im Menü **Start** den Befehl **Ausführen** klicken, im eingeblendeten Fenster eine Zeichenfolge der Form `ping <Computername>` eingeben und die Taste **Eingabe** drücken.

Wenn Sie eine Rückmeldung von Computer A erhalten, gehen Sie zum Schritt **9** weiter. Falls keine Rückmeldungen registriert werden, überprüfen Sie die Korrektheit der Parameter für die Verbindung zum Internet, die Richtigkeit der angegebenen IP-Adresse und des Computernamens.

9 Starten Sie den Drucker-Installationsassistenten.

10. Wählen Sie die Option **Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist** (**A network printer, or a printer attached to another computer**) und klicken dann auf **Weiter** (**Next**).
11. Geben Sie im Feld Verbindung mit dem Drucker herstellen (Connect to this printer) eine Zeichenfolge der folgenden Form ein: `\\<Computername>\<Freigegebener Druckerordner>`. In unserem Beispiel könnte die Zeichenfolge so aussehen: `\\pc15\Printer`.
12. Klicken Sie auf **Weiter** (**Next**) und warten, bis alle benötigten Treiber von Computer A auf Computer B kopiert sind (die Wartezeit kann über 20 Minuten in Anspruch nehmen).
13. Schließen Sie die Druckerinstallation auf die übliche Art und Weise ab.

Nach Durchführung der oben aufgezählten Schritte können nun Dokumente von Computer B an den Drucker, der an Computer A angeschlossen ist, zum Drucken gesendet werden.

3

Tunnelung von Knoten, die sich nicht im Subnetz des tunnelnden Coordinators befinden

Bei der Planung des betrieblichen ViPNet Netzwerks kann die Notwendigkeit entstehen, Knoten zu tunneln, die sich in einem separaten Segment des lokalen Netzwerks befinden, in welchem kein Coordinator installiert ist. Diese Aufgabe kann durch zusätzliche Einstellungen auf dem Coordinator gelöst werden, allerdings unter der Bedingung, dass Verbindungen zu getunnelten Knoten von geschützten ViPNet Knoten initiiert werden.

Betrachten wir das nachfolgende Schema.

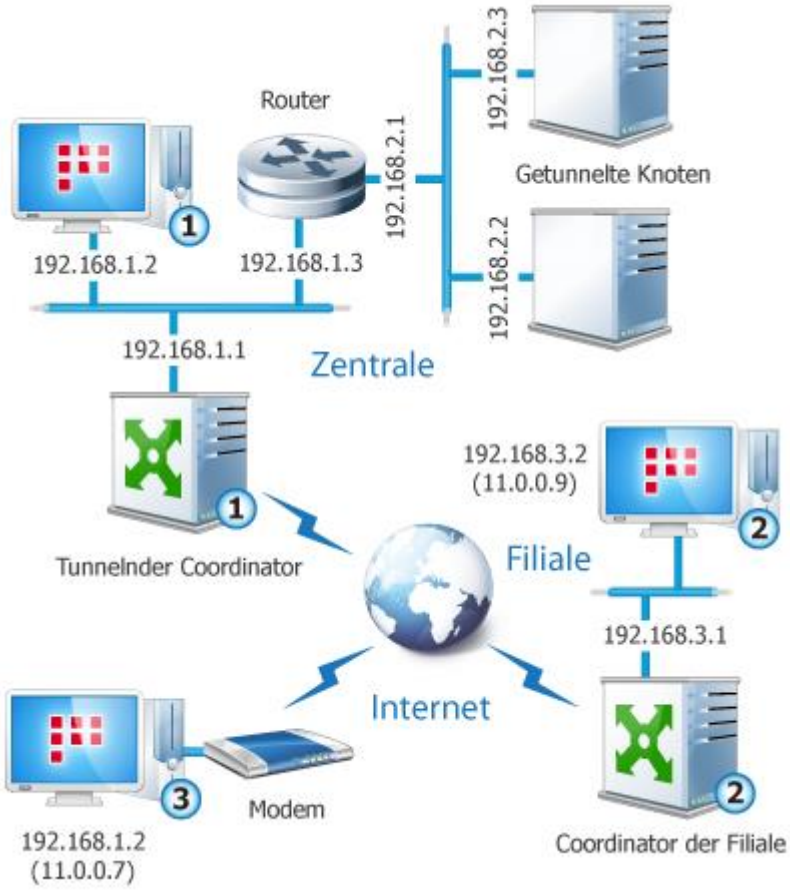

Abbildung 2. Tunnelung von Knoten, die sich im separaten Subnetz befinden

In dem Schema ist ein ViPNet Netzwerk abgebildet, das Computer in der Zentrale, Computer in der Filiale sowie Computer von entfernten ViPNet Benutzern umfasst. In der Zentrale ist ein Coordinator 1 installiert, bei welchem ein Netzwerkadapter an das Internet und der zweite Netzwerkadapter an das lokale Büronetzwerk angeschlossen ist. Zusätzlich befinden sich in der Zentrale mehrere ungeschützte Server (ohne installierter ViPNet Software), die aus Sicherheitsgründen in einem separaten Netzwerksegment untergebracht sind. Das Routing zwischen dem Netzwerksegment, in dem sich ungeschützte Server befinden, und dem Segment, in dem der Coordinator aufgestellt ist, ist implementiert.

Für ViPNet Netzwerkbenutzer in der Filiale sowie für entfernte Benutzer muss ein geschützter Zugang zu den Servern bereitgestellt werden. Das heißt, mit Hilfe des Coordinators 1 muss die Tunnelung ungeschützter Server eingerichtet werden. Normalerweise wird es empfohlen, den tunnelenden Coordinator an der Grenze des Segments aufzustellen, in welchem sich die getunnelten Knoten befinden. In unserem Fall ist der Coordinator 1 durch eine Firewall von den getunnelten Objekten getrennt.

Wenn der Coordinator 1 ein IP-Paket vom geschützten ViPNet Knoten an den getunnelten Knoten übermittelt, wird als Quell-IP-Adresse die sichtbare Adresse des geschützten Knotens (oft virtuell) angegeben. Antwortpakete von getunnelten Knoten werden an diese Adressen weitergeleitet, können aber innerhalb der vorgegebenen Netzwerkstruktur (s. Abbildung 2 auf S. 17) die Firewall nicht passieren. Um dieses Problem zu lösen, sollte auf dem Coordinator 1 eine Quellübersetzungsregel definiert werden, sodass IP-Pakete im Namen des Coordinators 1 an die getunnelten Knoten weitergeleitet werden. In

diesem Fall können Verbindungen erfolgreich aufgebaut werden, allerdings unter der Bedingung, dass ein geschützter ViPNet Knoten als Initiator auftritt.

Führen Sie die folgenden Schritte aus, um die Tunnelung ungeschützter Server mit Hilfe des Coordinators 1, der sich in einem anderen Netzwerksegment befindet, zu organisieren:

1 Wählen Sie im Programm ViPNet Network Manager den tunnelnden Coordinator aus und geben in der Registerkarte **Tunnel** die IP-Adressen der getunnelten Knoten an (in unserem Beispiel 192.168.2.2, 192.198.2.3).

2 Erstellen Sie im Programm ViPNet Network Manager neue Schlüsseldistributionen und versenden diese an die Netzwerkknoten.

3 Konfigurieren Sie auf dem tunnelenden Coordinator im Programm ViPNet Monitor eine Regel für die Adressübersetzung:

3.1 Wählen Sie im Hauptfensterfenster von ViPNet Coordinator in der Navigationsleiste den Bereich **Netzwerkfilter** > **NAT-Regeln**. Klicken Sie dann auf **Erstellen**.

3.2 Geben Sie im Fenster der Optionen für NAT-Regeln im Bereich **Allgemeine Optionen** den Namen der neuen Regel ein.

3.3 Geben Sie im Bereich **Quellen** mit Hilfe der Schaltfläche **Hinzufügen** die sichtbaren IP-Adressen von ViPNet Netzwerkknoten ein, die Zugang zu den getunnelten Knoten erhalten sollen.

Beispiel: Client 1 (s. Abbildung 2 auf S. 17) besitzt die IP-Adresse 192.168.1.2. Für die Clients 2 und 3 werden auf dem tunnelenden Coordinator die virtuellen IP-Adressen 11.0.0.9 und 11.0.0.7 verwendet. Diese IP-Adressen sollten also im Bereich **Quellen** angegeben werden.

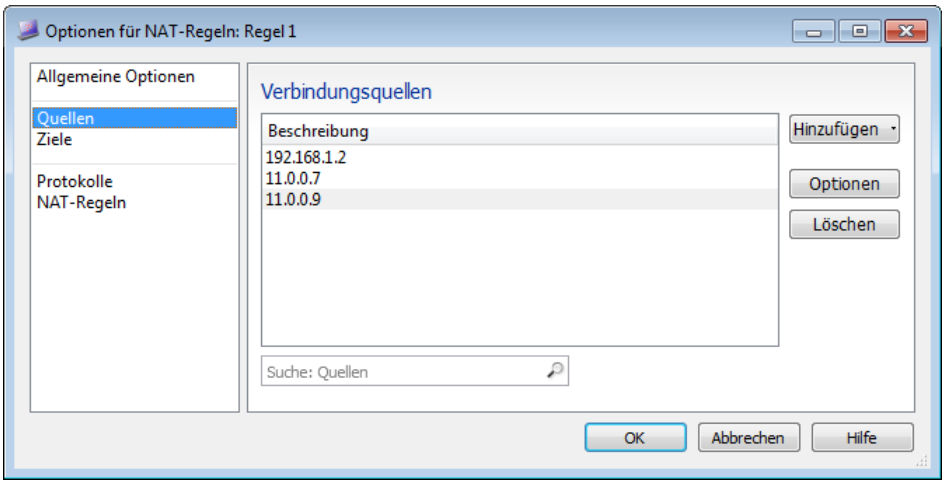

Abbildung 3. Quell-Adressen angeben

3.4 Aktivieren Sie im Bereich NAT-Regeln das Kontrollkätschen **Quelladresse ersetzen durch** und wählen **IP-Adresse des ausgehenden Netzwerkadapter (wird automatisch festgelegt)**.

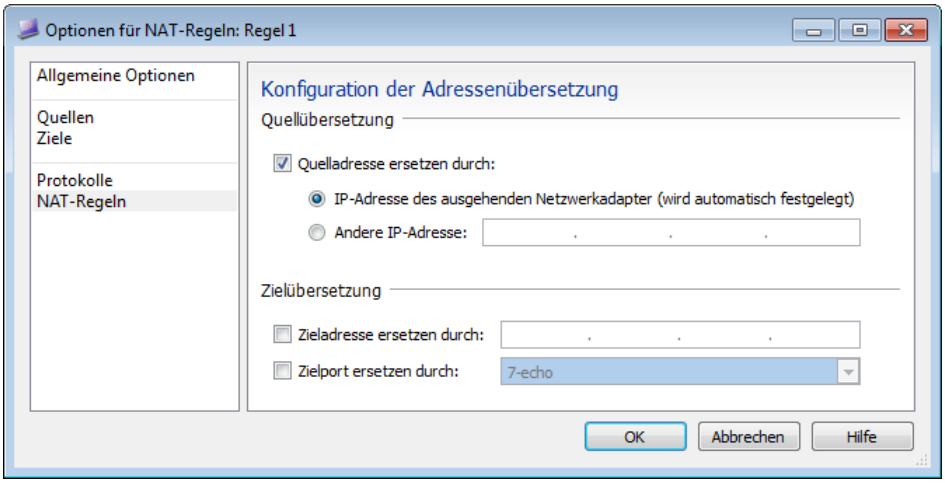

Abbildung 4. Parameter der NAT-Regel definieren

3.5 Klicken Sie auf **OK**.

Nach Durchführung der oben aufgezählten Einstellungen werden die Server für die geschützten ViPNet Knoten erreichbar sein. Die Vorteile dieser Vorgehensweise bestehen darin, dass keine Systemeinstellungen auf den getunnelten Knoten geändert und keine zusätzlichen Regeln auf der Firewall, die sich an der Grenze des betroffenen Netzwerksegments befindet, konfiguriert werden müssen.

4

Besonderheiten einer integrierten Firewall

Allgemeine Informationen 21

Einsatz der integrierten Firewall 22

Konfiguration der Netzwerkfilter zum Durchlassen des Traffics 23

Konfiguration der Netzwerkfilter für Clients 25

Konfiguration der Netzwerkfilter für Coordinatoren 29

Allgemeine Informationen

Um einen an ein Netzwerk angeschlossenen Rechner vor einen unbefugten Zugriff und Installation von schädlichen Softwarekomponenten zu schützen, muss man den gesamten offenen, geschützten und getunnelten Traffic kontrollieren. Zur Filterung des offenen Datenverkehrs, der die meisten Gefahren mit sich bringt, werden Firewalls eingesetzt (z.B. Windows Firewall). Auf den geschützten ViPNet Netzwerkknoten kann man außerdem die in den Programmen ViPNet Client und ViPNet Coordinator integrierten Firewalls verwenden. Das Programm ViPNet Client stellt die Funktionen einer für jedes Benutzerkonto separat konfigurierbaren Firewall. Das Programm ViPNet Coordinator agiert selbst als eine Firewall, indem es offene lokale und Transitverbindungen anhand von bestimmten Regeln filtert, sowie die Übersetzung der IP-Adressen (die NAT-Funktion) für das durchgehende Traffic übernimmt.

Standardmäßig verfügen die Clients und Coordinatoren eines ViPNet Netzwerks über voreingestellte Netzwerkfilter, die den gesamten offenen Traffic durchlassen, d.h. die integrierte ViPNet VPN Firewall ist deaktiviert. Das beugt Konfliktsituationen und Internetzugangsstörungen vor, im Fall wenn auf dem Knoten eine andere Firewall aktiviert ist (z.B. Windows Firewall). Windows Firewall ist ein Bestandteil des Windows Betriebssystems, sie ist standardmäßig aktiviert und wird weder bei der Installation vom ViPNet Client noch von ViPNet Coordinator automatisch deaktiviert.

Einsatz der integrierten Firewall

Die in der ViPNet VPN Software integrierten Firewall-Funktionen ermöglichen eine an Ihre Zwecke angepasste Verwaltung des offenen Traffics. Sie können Filter erstellen, die bestimmte IP-Pakete aus dem offenen Netzwerk durchlassen oder blockieren, und folgende Parameter einstellen:

- Quelle- und Zieladressen des IP-Pakets;
- Filterung der IP-Pakete anhand Protokolle;
- Zeitplan.

Außerdem können Sie mit Hilfe der ViPNet VPN Software die für das offene Netzwerk erstellten Filter zentralisiert auf die geschützten Netzwerkknoten anwenden. Dafür wird das Programm ViPNet Policy Manager eingesetzt, mit dessen Hilfe Sie Netzwerkfilter und NAT-Regeln erstellen und danach als Teil einer Sicherheitsrichtlinie an Knoten Ihres ViPNet VPN Netzwerkes übertragen können. Die vom ViPNet Policy Manager abgeschickten Filter und Regeln werden auf den Clients und Coordinatoren des Netzwerks automatisch angewendet. Sie sind nicht editierbar, haben einer höhere Priorität und werden deswegen als Erstes ausgeführt. Wir empfehlen Ihnen die Sicherheitsrichtlinien im Programm ViPNet Policy Manager zu verwalten (detaillierte Anleitung dafür finden Sie im Dokument „ViPNet Policy Manager. Administratorhandbuch"). Sollte das Programm ViPNet Policy Manager nicht im Einsatz sein, können Sie Ihre eigenen Netzwerkfilter in den Programmen ViPNet Client und ViPNet Coordinator erstellen.

Folgende Möglichkeiten stehen Ihnen bei der Verwendung der integrierten ViPNet VPN Firewall zur Verfügung:

1. Den unerwünschten Traffic blockieren (wird empfohlen). Führen Sie hierfür folgende Aktionen durch:
   - Erstellen Sie Ihre eigenen Filter, die den unerwünschten Traffic blockieren. Detaillierte Anleitung dafür finden Sie in den Abschnitten Konfiguration der Netzwerkfilter für Clients (auf S. 25) und Konfiguration der Netzwerkfilter für Coordinatoren (auf S. 29).
   - Setzen Sie die integrierte ViPNet VPN Firewall parallel zu anderen Firewalls ein.
2. Den gesamten offenen Traffic blockieren und nur bestimmten Traffic erlauben.

Achtung! Diese Methode sollte nur von erfahrenen Administratoren verwendet werden.

Dafür machen Sie folgendes:

- Löschen Sie den Standardfilter, der den gesamten offenen Traffic erlaubt. Der Filter, welcher den gesamten Traffic blockiert, wurde bereits bei der Programminstallation automatisch angelegt und ist nicht editierbar.
- Erstellen Sie Ihre eigenen Filter, die den notwendigen Traffic erlauben und deaktivieren alle anderen Firewalls (einschließlich der Windows Firewall). Mehr dazu im Abschnitt Konfiguration der Netzwerkfilter zum Durchlassen des Traffics (auf S. 23).

Konfiguration der Netzwerkfilter zum Durchlassen des Traffics

Bevor Sie eigene Filter zum Durchlassen des offenen Traffics auf einem Client oder Coordinator eines ViPNet Netzwerkes erstellen, führen Sie folgende Aktionen durch:

- Löschen oder deaktivieren Sie den Standardfilter, der den gesamten offenen Traffic erlaubt.
- Deaktivieren Sie alle anderen Firewalls, auch die Windows Firewall (mehr dazu finden Sie auf der Internetseite von Microsoft http://windows.microsoft.com/de-de/windows/turn-windows-firewall-on-off#turn-windows-firewall-on-off=windows-7).

Jetzt können Sie Ihre eignen Filter erstellen, die den gewünschten Traffic aus offenen Netzwerken durchlassen (siehe Abschnitte Konfiguration der Netzwerkfilter für Clients (auf S. 25) und Konfiguration der Netzwerkfilter für Coordinatoren (auf S. 29)). Es wird außerdem empfohlen, die unten beschriebenen und nach ihrer Priorität sortierten Filter anzulegen.

Die für Coordinatoren eines ViPNet Netzwerkes empfohlenen Filter erlauben alle IP-Pakete folgender Arten des Traffics:

- DHCP-Traffic, der die Zuteilung einer IP-Adresse und anderer Parameter dem Knoten ermöglicht, welche für die Kommunikation innerhalb eines TCP/IP-Netzwerks notwendig sind.

Hinweis. Der Filter für den DHCP-Traffic wird nur benötigt, wenn im Netz ein DHCP-Server verwendet wird.

- NetBIOS-Traffic, der in lokalen Netzwerken den Zugriff auf eigene lokalen Ressourcen und Ressourcen von Remoterechnern ermöglicht.
- Traffic des WINS-Diensts. Dieser Dienst wandelt die IP-Adressen in NetBIOS-Namen um und vereinfacht somit die Verwaltung der NetBIOS-Namespaces in TCP/IP-Netzwerken.

Auf diese Weise übernimmt ein Coordinator die Funktionen einer Firewall, die die Sicherheit der Kommunikationskanale zwischen Netzwerkknoten und externen Computern (z.B. beim Zugriff auf Internetressourcen aus einem lokalen Netzwerk) gewährleistet.

Tabelle 3. Empfohlene Einstellungen für Filter des offenen Netzwerks auf einem ViPNet VPN Coordinator

Aktion	Name	Quelle	Ziel	Protokoll
Erlauben	DHCP-Traffic	Alle	Alle	DHCP (UDP: von 67 auf 68, von 68 auf 67)
Erlauben	NetBIOS- und WINS-Traffic	Alle	Alle	NetBIOS-DGM (UDP: von 138 auf 138) NetBIOS-NC (UDP: von 137 auf 137)

Die oben beschriebenen Empfehlungen gelten gleichermaßen für einen Coordinator als auch für einen ViPNet VPN Client. Außerdem empfehlen wir auf einem Client einen Filter anzulegen, der den gesamten ausgehenden Traffic eines Knotens in ein offenes Netz erlaubt. Somit erlaubt die integrierte Firewall alle ausgehenden und beschränkt die eingehenden Anfragen auf einem ViPNet VPN Client.

Tabelle 4. Empfohlene Einstellungen für Filter des offenen Netzwerks auf einem ViPNet VPN Client

Aktion	Name	Quelle	Ziel	Protokoll
Erlauben	DHCP-Traffic	Alle	Alle	DHCP (UDP: von 67 auf 68, von 68 auf 67)
Erlauben	NetBIOS- und WINS-Traffic	Alle	Alle	NetBIOS-DGM (UDP: von 138 auf 138) NetBIOS-NC (UDP: von 137 auf 137)
Erlauben	Ausgehender Traffic	Mein ViPNet Knoten	Alle	Alle

Konfiguration der Netzwerkfilter für Clients

Für die Clients eines ViPNet VPN Netzwerks empfehlen wir eine zentralisierte Filterverwaltung im Programm ViPNet Policy Manager. Dadurch ersparen Sie sich als Netzwerkadministrator die Einzelkonfigurationen auf jedem Knoten, die vor allem bei einer großen Anzahl an Clients sehr zeitintensiv sein kann. Eine detaillierte Anleitung zur Verwaltungen der Netzwerkknoten-Sicherheitsrichtlinien im Programm ViPNet Policy Manager finden Sie im Dokument „ViPNet Policy Manager. Administratorhandbuch".

Sollte das Programm ViPNet Policy Manager nicht im Einsatz sein, können Sie die Netzwerkfilter für die Clients Ihres ViPNet VPN Netzwerks manuell anlegen. Standardmäßig wird dafür das Programm ViPNet Monitor mit einer vereinfachten Benutzerschnittstelle verwendet. Im Administratormodus stehen Ihnen die erweiterten Programmeinstellungen (einschließlich die Konfiguration von Netzwerkfiltern) zur Verfügung. Dafür benötigen Sie das Passwort des ViPNet Knotenadministrators, welches Sie dem Programm ViPNet Network entnehmen können. Öffnen Sie dafür im Bereich **Eigenes Netzwerk** die Registerkarte **Passwörter**.

Abbildung 5. Passwort des Netzwerkknotenadministrators im ViPNet Network Manager anzeigen

Eine detaillierte Anleitung zum Arbeiten im ViPNet Client mit Administratorrechten finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch" im Abschnitt „Arbeiten mit dem Programm im Administratormodus".

So erstellen Sie einen Filter des offenen Netzwerks im Programm ViPNet Client:

1 Melden Sie sich im Programm als Administrator an.

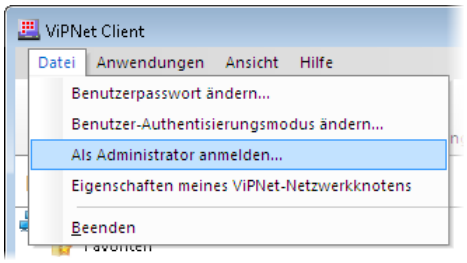

Abbildung 6. Als Administrator anmelden

2 Wählen Sie in der Navigationsleiste den Bereich **Netzwerkfilter** > **Filter des offenen Netzwerks** aus.

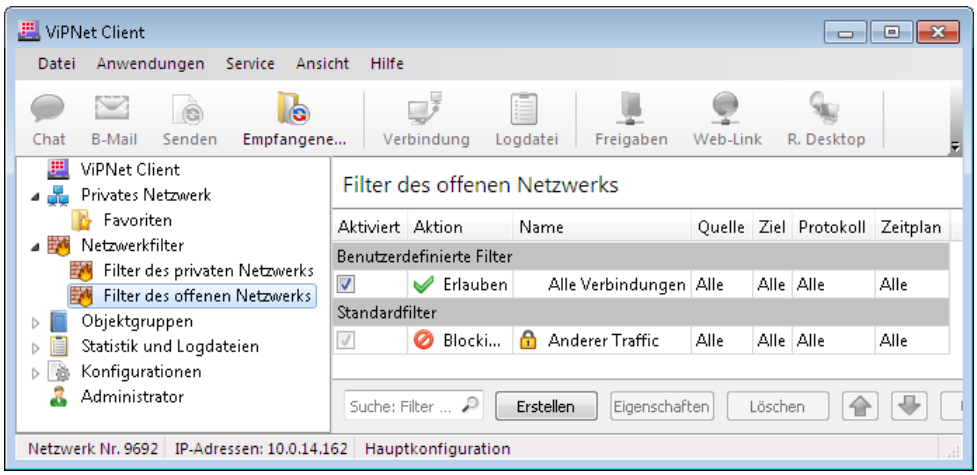

Abbildung 7. Standardfilter des offenen Netywerks in ViPNet Client

3 Klicken Sie in der Panel-Ansicht auf die Schaltfläche **Erstellen**.

4 Geben Sie im geöffneten Fenster im Bereich **Allgemeine Optionen** eine Filterbezeichnung an und definieren, ob er den Traffic erlauben oder blockieren soll.

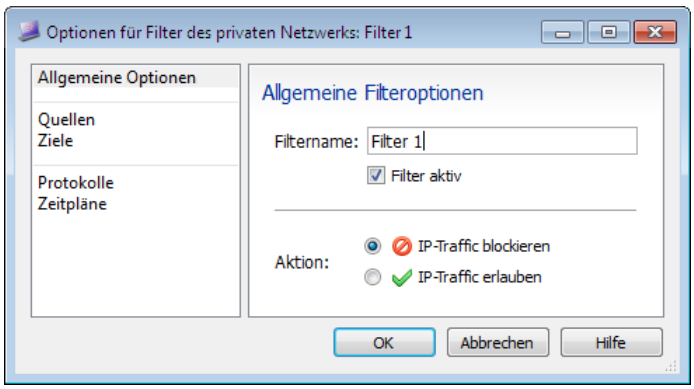

Abbildung 8. Definition allgemeiner Parameter für Filter

5 Geben Sie im Bereich **Quellen** den Absender der offenen IP-Pakete an. Damit der Filter nur auf die ausgehenden offenen Verbindungen Ihres Knotens angewendet wird, wählen Sie **Mein ViPNet Knoten** aus. Wenn Sie keinen Absender angeben, wird der Filter auf alle IP-Pakete von jeder beliebigen Quelle (auch von Ihrem Knoten) angewendet.

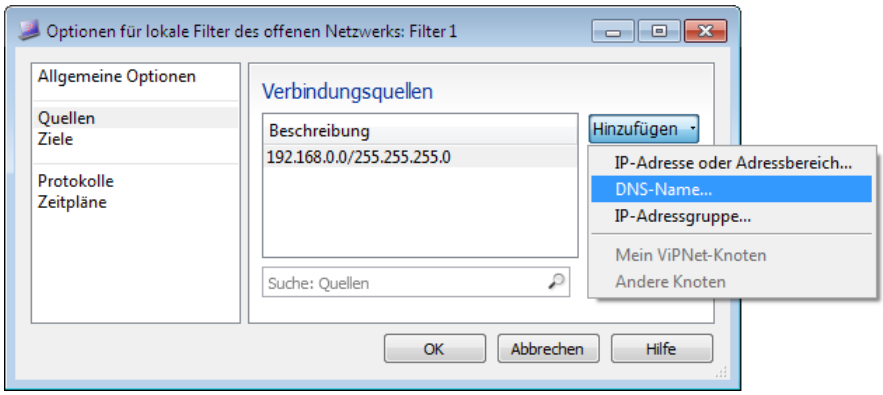

Abbildung 9. Definition der Absender offener IP-Pakete

Hinweis. Um die Erstellung von Netzwerkfiltern im Programm ViPNet Client zu erleichtern, können Sie mit Objektgruppen arbeiten. Mehr dazu finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch“ im Bereich „Integrierte Firewall“.

6 Geben Sie im Bereich **Ziel** den Empfänger der IP-Pakete an, sonst wird der Filter auf alle an einen beliebigen offenen Knoten verschickten IP-Pakete angewendet.

7 Geben Sie im Bereich **Protokolle** den Protokoll oder die Gruppe von Protokollen an, der/die gefiltert werden soll (z.B. DHCP).

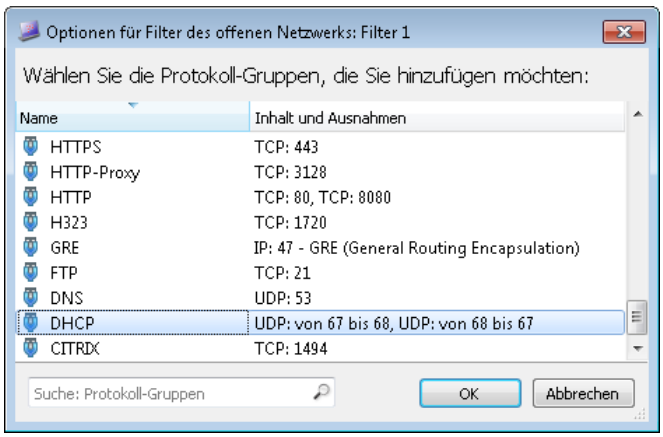

Abbildung 10. Protokoll-Gruppe definieren

8 Bei Bedarf geben Sie im Bereich **Zeitpläne** an, wann der Filter ausgeführt werden soll (Datum und Uhrzeit).

9 Um die Erstellung des Filters abzuschließen, klicken Sie auf **OK**. In der Panel-Ansicht erscheint nun der neu angelegte Filter.

10 Wiederholen Sie die Schritte 3 bis 9, um einen weiteren Filter zu erstellen.

11 Definieren Sie die Prioritäten einzelner Filter, indem Sie ihre Reihenfolge in der Liste Benutzerdefinierte Filter mit den Schaltflächen und anpassen:

- Wenn Sie Filter erstellt haben, die den unerwünschten Traffic blockieren, ordnen Sie sie nach ihrer Priorität vor dem Filter Alle Verbindungen ein.

- Wenn Sie Filter erstellt haben, die den erwünschten Traffic erlauben, wählen Sie den Standardfilter **Alle Verbindungen** aus und löschen ihn mit der Schaltfläche **Löschen**. Die Reihenfolge der empfohlenen Filter zum Durchlassen vom Traffic stellen Sie entsprechend der im Anschnitt Konfiguration der Netzwerkfilter zum Durchlassen des Traffics (auf S. 23) angeführten Tabelle. Nach der Konfiguration der Filter zum Durchlassen vom Traffic deaktivieren Sie alle anderen Firewalls.

12 Klicken Sie in der Panel-Ansicht auf die Schaltfläche **Übernehmen** und bestätigen die Änderungen, um die erstellen Filter zu aktivieren.

Konfiguration der Netzwerkfilter für Coordinatoren

Für die Coordinatoren eines ViPNet Netzwerks empfehlen wir eine zentralisierte Filterverwaltung im ViPNet Policy Manager Programm. Detaillierte Informationen zu Verwaltung der Sicherheitsrichtlinien von ViPNet Netzwerkknoten entnehmen Sie dem Dokument "ViPNet Policy Manager. Administratorhandbuch".

Sollte das Programm ViPNet Policy Manager nicht im Einsatz sein, können Sie lokale und Transitfilter des offenen Netzwerks sowie NAT-Regeln im Programm ViPNet Coordinator erstellen. Die lokalen Filter des offenen Netzwerks legen Sie im Bereich **Netzwerkfilter** > **Lokale Filter des offenen Netzwerks** an. Auf den Coordinatoren sind standardmäßig Filter eingerichtet, die den gesamten offenen Traffic durchlassen. Das Vorgehen beim Anlegen eines lokalen Filters auf einem Coordinator und einem Client (s. Konfiguration der Netzwerkfilter für Clients auf S. 25) ist bis auf die Einstellungsmöglichkeiten für Netzwerkadapter gleich: Auf einem Coordinator im Einstellungsfenster in den Bereichen **Quellen** und **Ziele** können neben den Quelle- und Zieladressen noch Netzwerkadapter eingestellt werden, die die IP-Pakete von den ausgewählten Absendern (Quellen) empfangen und an die angegebenen Empfänger (Ziele) schickten sollen.

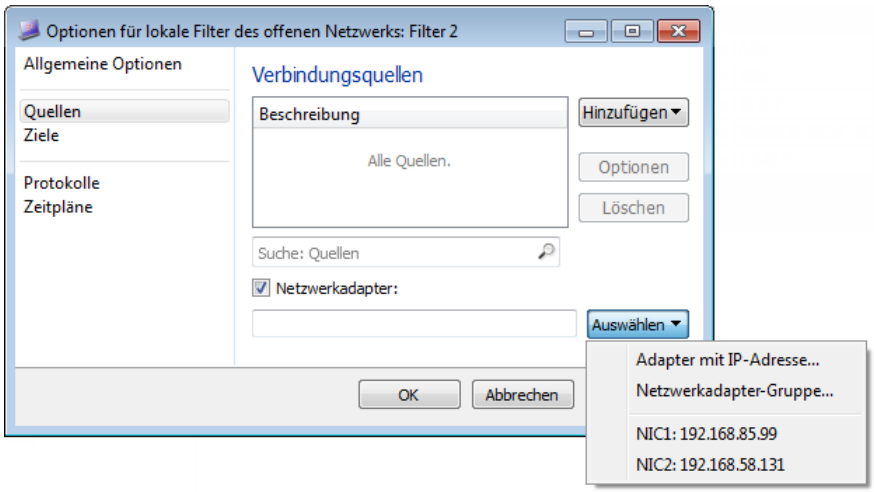

Abbildung 11. Definieren des Quell-Netzwerkadapters in ViPNet Coordinator

Die NAT-Regeln richten Sie im Bereich **Netzwerkknoten** > **NAT-Regeln** ein. Sie werden auf dem Coordinator angewendet, der das lokale und das globale Netz voneinander abgrenzt, um die zwei grundliegenden Aufgaben zu lösen:

- Wenn eine Verbindung des lokalen Netzwerks mit dem Internet nötig ist, wobei die Anzahl der Knoten im lokalen Netzwerk die Anzahl der vom Provider bereitgestellten öffentlichen IP-Adressen überschreitet.
- Für den Zugang zu internen Ressourcen aus einem öffentlichen Netzwerk.

In diesem Bereich gibt es keine vordefinierten Einstellungen. Detaillierte Anleitung zum Anlegen der NAT-Regeln finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch“ im Abschnitt „Übersetzung von IP-Adressen (NAT)“.

Als Ergänzung zu den NAT-Regeln sollten im Bereich **Netzwerkfilter** > **Transit-Filter des offenen Netzwerks** Transit-Filter des offenen Netzwerks eingerichtet werden. Sie erlauben den Traffic zwischen Segmenten des lokalen Netzwerks und dem Internet in die angegebenen Richtungen. Standardmäßig sind diese Filter nicht vorhanden, Sie können sie aber analog den lokalen Filtern des offenen Netzwerks einrichten.

5

Beispiel für die Verwaltung von Netzwerkknoten-Sicherheitsrichtlinien mit Hilfe von ViPNet Policy Manager

In diesem Abschnitt ist ein Beispiel für die Verwendung des Programms ViPNet Policy Manager für die zentralisierte Verwaltung von Sicherheitsrichtlinien der ViPNet Netzwerkknoten aufgeführt.

Nehmen wir an, es soll ein Filter erstellt werden, der den Zugriff von Clients auf die Webseiten unterschiedlicher sozialer Netzwerke blockiert. Das Erstellen eines solchen Filters im Programm ViPNet Policy Manager und das Versenden des Filters an die ViPNet Netzwerkknoten ermöglicht es dem Administrator, die manuelle Konfiguration der Einstellungen auf jedem einzelnen Knoten zu vermeiden. Auf den Netzwerkknoten tritt der Filter automatisch in Kraft, seine Parameter können dabei nicht bearbeitet werden.

Führen Sie zum Erstellen eines Filters, der den Zugang zu sozialen Netzwerken blockieren soll, im Programm ViPNet Policy Manager auf dem Manager-Arbeitsplatz die folgenden Schritte aus:

1. Wählen Sie in der Navigationsleiste den Bereich **Richtlinienvorlagen**.
2. Klicken Sie in der Panel-Ansicht auf die Schaltfläche **Erstellen**.
3. Geben Sie im eingeblendeten Fenster der Vorlageneigenschaften im Bereich **Allgemeine Optionen** den Namen der neuen Vorlage an.
4. Wählen Sie in der Navigationsleiste den Bereich **Lokale Filter des offenen Netzwerks** und klicken in der Panel-Ansicht auf die Schaltfläche **Erstellen**.

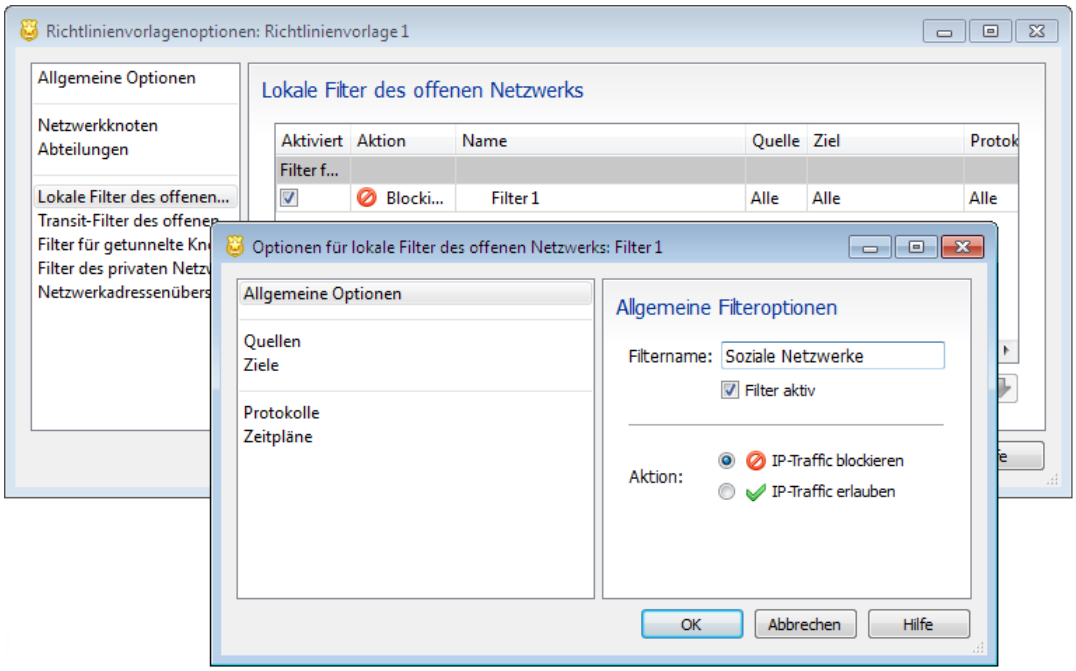

Abbildung 12. Erstellen des lokalen Filters des offenen Netzwerks für eine Sicherheitsrichtlinienvorlage

5 Geben Sie im eingeblendeten Fenster der Eigenschaften des lokalen Filters im Bereich **Allgemeine Optionen** den Namen des Filters und seine primäre Aktion an: **IP-Traffic blockieren** (diese Aktion ist standardmäßig ausgewählt).

6 Klicken Sie im Bereich **Quellen** auf die Schaltfläche **Hinzufügen** und wählen im Menü den Eintrag **Mein ViPNet Knoten**.

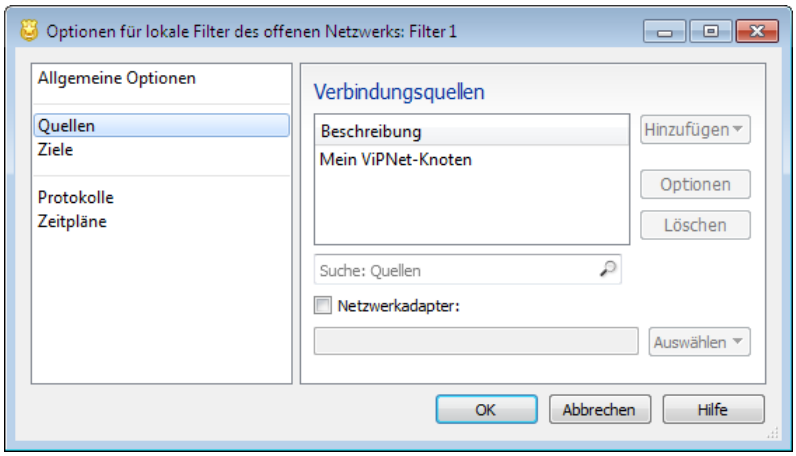

Abbildung 13. Festlegen der Verbindungsquelle

7 Klicken Sie im Bereich Ziele auf die Schaltfläche **Hinzufügen** und wählen im Menü den Eintrag **DNS-Name**.

8 Geben Sie im eingeblendeten Fenster **DNS-Name** den DNS-Namen des Servers des sozialen Netzwerks ein, zu welchem der Zugriff gesperrt werden soll, und klicken dann auf **OK**.

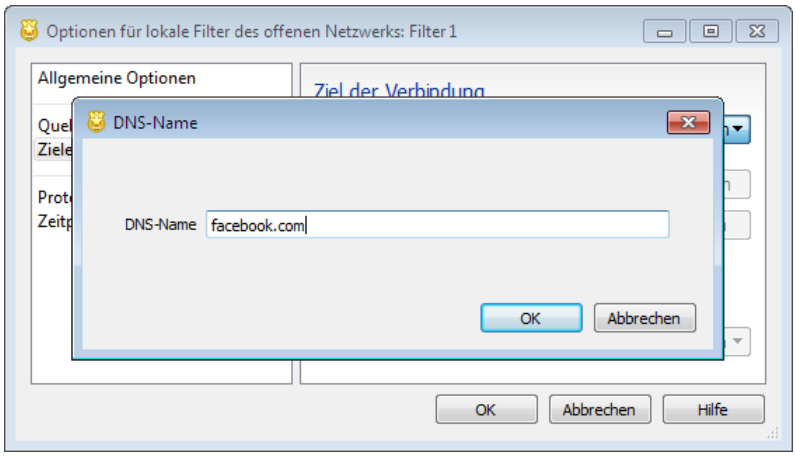

Abbildung 14. Festlegen des Verbindungsziels

9 Wiederholen Sie die Schritte **6–8** für die Server aller sozialen Netzwerke, die vom Filter erfasst werden sollen.

10 Klicken Sie im Fenster der Eigenschaften des lokalen Filters auf **OK**.

11 Wählen Sie im Fenster der Vorlageneigenschaften in der Navigationsleiste den Bereich **Netzwerkknoten**.

12 Klicken Sie in der Panel-Ansicht auf die Schaltfläche **Hinzufügen**.

13 Wählen Sie im eingeblendeten Fenster **Netzwerkknoten** alle Clients aus, auf welche die gegebene Vorlage angewendet werden soll, und klicken dann auf **OK**.

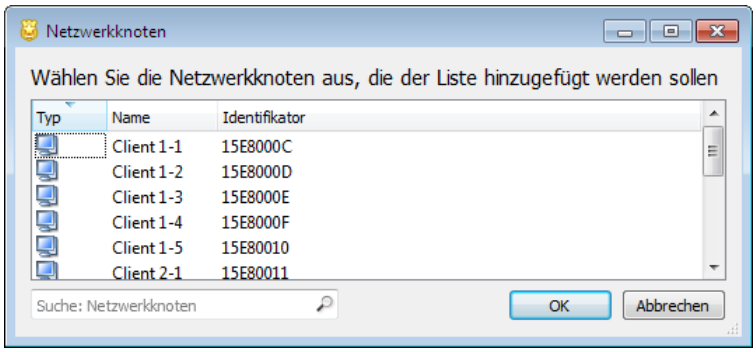

Abbildung 15. Wahlweises Hinzufügen von Netzwerkknoten

14 Klicken Sie im Fenster der Eigenschaften der Vorlage auf **OK**.

15 Wählen Sie im Hauptfenster von ViPNet Policy Manager den Bereich **Netzwerkknoten**. Wählen Sie innerhalb des Bereichs alle Knoten mit dem Richtlinienstatus **Verteilung erforderlich** aus.

16 Klicken Sie auf die Schaltfläche **Richtlinien verteilen**.

17 Behalten Sie im Fenster **Richtlinie verteilen** die standardmäßig eingetragenen Werte bei oder geben Sie die Zeit an, zu welcher die gesendeten Richtlinien in Kraft treten sollen.

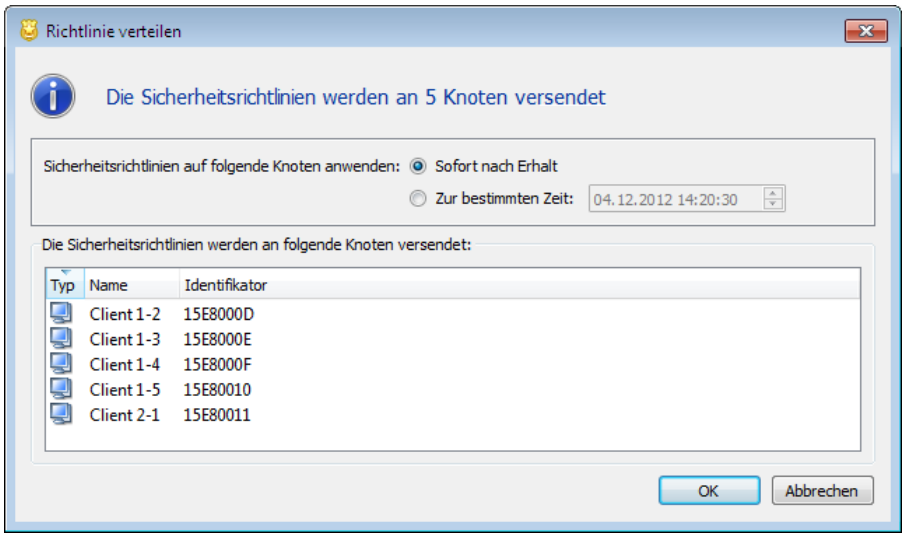

Abbildung 16. Verteilung von Sicherheitsrichtlinien an die Netzwerkknoten

18 Klicken Sie auf **OK**.

Im Hauptfenster von ViPNet Policy Manager im Bereich **Netzwerkknoten** ändert sich der Status der abgesendeten Richtlinien auf **Gesendet**. Sobald die Richtlinie für einen bestimmten Knoten an diesen Knoten erfolgreich zugestellt wurde, erhält diese Richtlinie den Status **An Knoten zugestellt**.

Der erstellte Filter wird im Programm ViPNet Client nach der Anmeldung im Administratormodus im Bereich **Filter des offenen Netzwerks** > **Filter für Sicherheitsrichtlinien** angezeigt.

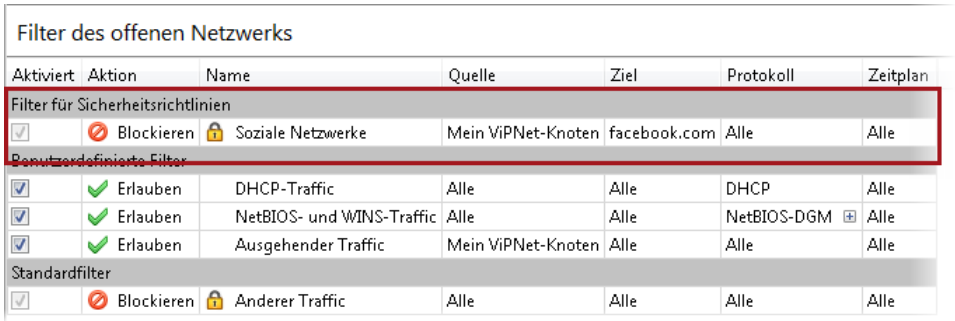

Abbildung 17. Filter der Sicherheitsrichtlinien in ViPNet Client

Ausführliche Informationen zur Verwendung des Programms ViPNet Policy Manager finden Sie im Dokument „ViPNet Policy Manager. Administratorhandbuch“.

6

Remote-Steuerung von ViPNet Netzwerkknoten

Automatische Anmeldung in Windows und ViPNet Software 36

Konfiguration des Terminalservers bei Remotesteuerung 41

Installation der Software für Remotesteuerung 43

Starten des Programms für die Remotesteuerung 44

Automatische Anmeldung in Windows und ViPNet Software

Wofür wird die automatische Anmeldung benötigt

Bei der Administration entfernter Computer oder Computer, auf die der physikalische Zugriff aus irgendwelchen Gründen nur schwer möglich ist, besteht oft die Notwendigkeit, nach einem Neustart des Rechners die Anmeldung im Betriebssystem und den Start des Programms ViPNet Monitor automatisch durchzuführen.

Wenn die Software ViPNet Client oder ViPNet Coordinator auf einem Server mit Betriebssystem Windows installiert ist, dann ist beim Start des Betriebssystems eine Benutzeranmeldung erforderlich. Dies ist dadurch bedingt, dass ViPNet Software (mit Ausnahme von ViPNet Treiber) als Anwendung und nicht als Dienst ausgeführt wird.

Damit auf einem Netzwerkknoten die Anmeldung im System und der Start des Programms ViPNet Monitor automatisch durchgeführt werden (ohne Benutzung der Tastatur und ohne physikalischen Zugriff), sollten Sie die folgenden Schritte ausführen:

- Erlauben Sie die automatische Anmeldung in den Systemeinstellungen von Windows (s. Konfiguration der automatischen Anmeldung in Windows auf S. 36).
- Speichern Sie das ViPNet Benutzerpasswort, das für den Zugang zu ViPNet Coordinator oder ViPNet Client verwendet wird (s. Automatische Anmeldung in ViPNet Software einstellen auf S. 39).

Konfiguration der automatischen Anmeldung in Windows

Zum Einstellen einer automatischen Anmeldung unter Windows:

1. Drücken Sie die Tastenkombination **Win+R**.

   Im Menü **Start** (**Start**) können Sie auch den Befehl **Ausführen** (**Run**) wählen.

2. Geben Sie im eingeblendeten Fenster im Feld **Öffnen** den Befehl `control userpasswords2` ein und klicken auf **OK**.

   Bei Verwendung von Windows Vista/Server 2008/Windows 7 können Sie auch den Befehl `netplwiz` verwenden.

3. Führen Sie im Fenster **Benutzerkonten** (**User Accounts**) in der Registerkarte **Benutzer** (**Users**) die folgende Aktionen durch:

   - Wählen Sie in der Registerkarte **Benutzer** (**Users**) den Benutzer in der Liste aus, unter wessen Konto die Anmeldung im Betriebssystem erfolgen soll, und deaktivieren das Kontrollkästchen

Benutzer müssen Benutzernamen und Kennwort eingeben (**Users must enter a username and password to use this computer**).

Der Benutzer muss in diesem Fall zur Gruppe **Administrators** gehören (Benutzer muss als Administrator des Computers registriert sein).

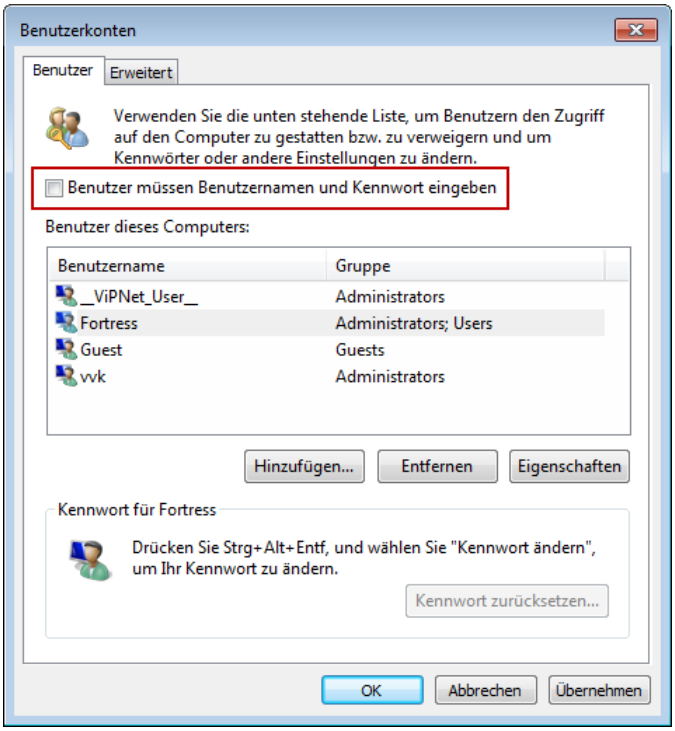

Abbildung 18. Automatische Anmeldung im Betriebssystem in der Registerkarte „Benutzer" konfigurieren

- Deaktivieren Sie in der Registerkarte **Erweitert** (**Advanced**) das Kontrollkästchen **Strg+Alt+Entf drücken ist für die Anmeldung erforderlich** (**Require users to press Ctrl+Alt+Delete**).

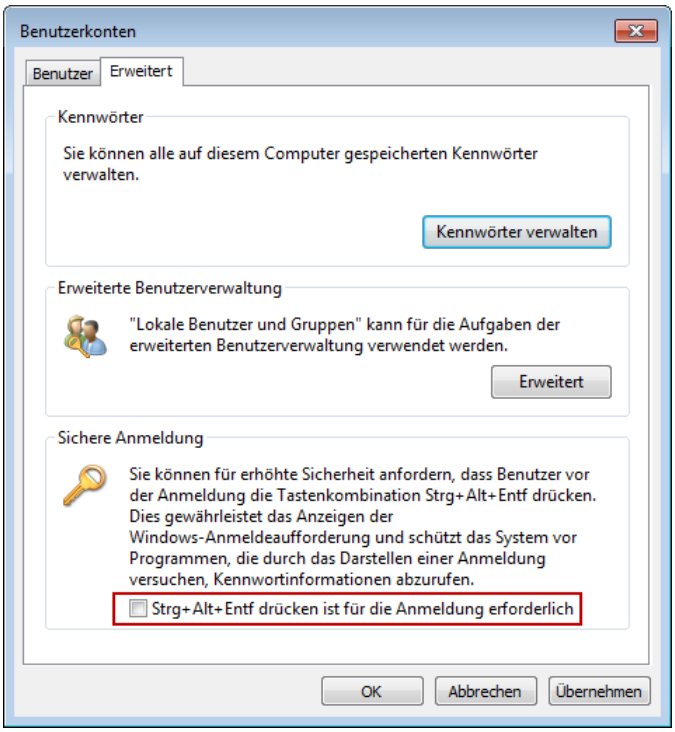
Benutzerkonten
Benutzer
Erweitert
Kennwörter
Sie können alle auf diesem Computer gespeicherten Kennwörter verwalten.
Kennwörter verwalten
Erweiterte Benutzerverwaltung
"Lokale Benutzer und Gruppen" kann für die Aufgaben der erweiterten Benutzerverwaltung verwendet werden.
Erweitert
Sichere Anmeldung
Sie können für erhöhte Sicherheit anfordern, dass Benutzer vor der Anmeldung die Tastenkombination Strg+Alt+Entf drücken. Dies gewährleistet das Anzeigen der Windows-Anmeldeaufforderung und schützt das System vor Programmen, die durch das Darstellen einer Anmeldung versuchen, Kennwortinformationen abzurufen.
Strg+Alt+Entf drücken ist für die Anmeldung erforderlich
OK
Abbrechen
Übernehmen

Abbildung 19. Automatische Anmeldung im Betriebssystem in der Registerkarte „Erweitert" konfigurieren

Hinweis. Wenn sich der Computer in einer Domäne befindet, können die angegebenen Kontrollkästchen aufgrund von Gruppensicherheitsrichtlinien fehlen oder nicht verfügbar sein. In diesem Fall ist zum Einstellen der automatischen Anmeldung im Betriebssystem die manuelle Bearbeitung der Registry erforderlich.

Unsachgemäße Bearbeitung der Registry kann zu Störungen in der Arbeit des Betriebssystems führen, deswegen sollte vor möglichen Eingriffen unbedingt eine Sicherungskopie der Registry erstellt werden. Die Kopie ermöglicht die Wiederherstellung der Registry im Fall von Problemen.

Wenn das Kontrollkästchen **Benutzer müssen Benutzernamen und Kennwort eingeben** (**Users must enter a username and password to use this computer**) fehlt oder nicht verfügbar ist, dann weisen Sie den Parametern im Registry-Bereich `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` die folgenden Werte zu:

- `AutoAdminLogon` – 1 („wahr"). Dieser Parameter wird dazu verwendet, die automatische Anmeldung im Betriebssystem zu aktivieren. Beim Setzen dieses Wertes auf `0` wird die auotmatishe Anmeldung deaktiviert.
- `DefaultDomainName` – Name der Domäne, in der sich der Computer des Benutzers befindet.
- `DefaultUserName` – Name des Benutzers, mit dessen Benutzerkonto die automatische Anmeldung im Betriebssystem erfolgen soll.
- `DefaultPassword` – Passwort des Benutzers. Wenn der Wert dieses Parameters nicht angegeben ist, wird der Parameter AutoAdminLogon automatisch wieder auf 0 („falsch") gesetzt, was eine automatische Anmeldung im Betriebssystem deaktiviert.

Wenn die angegebenen Parameter fehlen, erzeugen Sie diese manuell, indem Sie den

Datentyp Zeichenfolge (**REG_SZ**) verwenden.

Wenn das Kontrollkästchen **Strg+Alt+Entf drücken ist für die Anmeldung erforderlich** (**Require users to press Ctrl+Alt+Del**) fehlt oder nicht verfügbar ist, dann weisen Sie dem Parameter `Disablecad` im Registry-Zweig `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Policies\System` den Wert 1 („wahr“) zu. Wenn dieser Parameter fehlt, erzeugen Sie diesen manuell, indem Sie den Typ **DWORD** verwenden.

- Klicken Sie auf **Übernehmen** (**Apply**).

4 Geben Sie im Fenster **Automatische Anmeldung** (**Automatically Log On**) das Passwort ein und klicken auf **OK**.

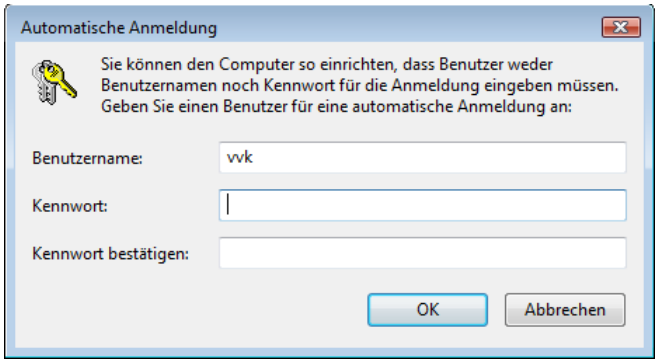
Automatische Anmeldung
Sie können den Computer so einrichten, dass Benutzer weder Benutzernamen noch Kennwort für die Anmeldung eingeben müssen. Geben Sie einen Benutzer für eine automatische Anmeldung an:
Benutzername:
vvk
Kennwort:
Kennwort bestätigen:
OK
Abbrechen

Abbildung 20. Fenster zur Passwort-Eingabe für die automatische Anmeldung im Betriebssystem

Bei nachfolgenden Starts des Computers wird die Anmeldung im Betriebssystem unter dem Konto des gewählten Benutzers ohne Eingabe eines Passworts und ohne Betätigung der Tastenkombination **Strg**+**Alt**+**Entf** durchgeführt.

Automatische Anmeldung in ViPNet Software einstellen

Damit der Netzwerkknotenauch im Fall eines außerplanmäßigen Systemneustarts verfügbar bleibt, sollte das Benutzerpasswort im System gespeichert werden. Führen Sie dazu die folgenden Schritte aus:

1 Stellen Sie sicher, dass im Hauptfenster des Programms ViPNet Network Manager auf der Registerkarte **Schlüssel** das Kontrollkästchen **Passwort darf gespeichert werden** für den betroffenen Netzwerkknoten aktiviert ist. Wenn dieses Kontrollkästchen deaktiviert ist, dann aktivieren Sie es und senden anschließend ein Schlüsselupdate an den Netzwerkknoten.

Abbildung 21. Aktivieren der Passwortspeicherung

Wenn das Speichern des Passworts im Programm ViPNet Network Manager erlaubt ist, dann wird das Kontrollkästchen **Passwort speichern** im Fenster zur Passworteingabe auf dem Netzwerkknoten standardmäßig aktiviert.

2 Starten Sie auf dem Netzwerkknoten die Software ViPNet Coordinator oder Client.

3 Geben Sie das ViPNet Benutzerpasswort ein.

4 Aktivieren Sie das Kontrollkästchen **Passwort speichern** (falls es nicht bereits aktiviert ist) und klicken auf **OK**.

Nach der Durchführung der aufgezählten Schritte wird die Benutzeranmeldung im Programm ViPNet Coordinator oder ViPNet Client beim Start des Servers automatisch durchgeführt (die Eingabe des Benutzerpassworts ist dabei nicht erforderlich).

Konfiguration des Terminalservers bei Remotesteuerung

Während der Arbeit in einer Terminal-Sitzung (z.B. bei Verbindungen zum Server mit Hilfe des Programms Remote Desktop Connection) kann die folgende Situation auftreten: beim Beenden der Terminal-Sitzung wird das Programm ViPNet Monitor automatisch aus dem Speicher des Remote-Servers entladen und der Schutz des IP-Traffics wird deaktiviert. Wenn dieses Problem auf einem Coordinator auftritt, dann kommt es auf allen ViPNet Netzwerkknoten, die diesen Coordinator als Firewall oder IP-Adressenserver verwenden, zu Störungen in der Verbindung.

Dieses Problem tritt auf, wenn der Terminal-Server so konfiguriert wurde, dass er alle Anwendungen des Benutzers nach seiner Anmeldung in der Sitzung beendet. In der folgenden Abbildung sind Einstellungen im Snap-In **RDP-Tcp Eigenschaften** aufgeführt, die zum unerwünschten Beenden des Programms ViPNet Monitor führen.

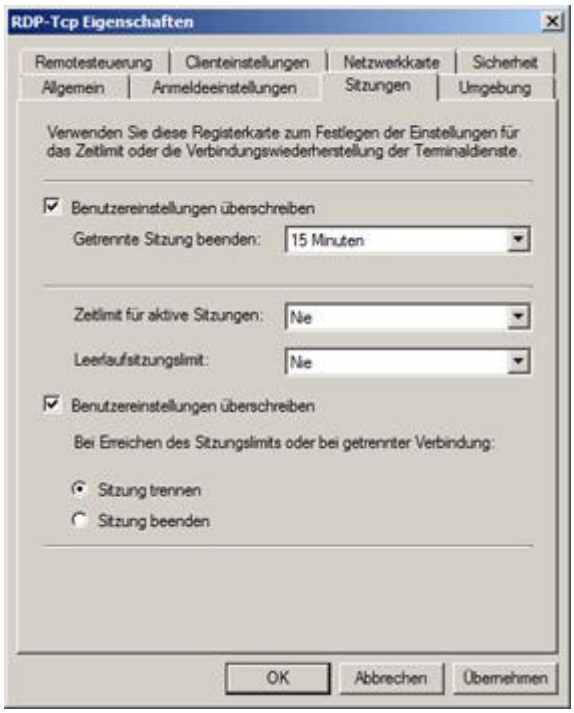

Abbildung 22. Fehlerhafte Einstellungen eines Terminal-Servers

Zur Lösung des Problems sollten alle Einstellungen durch das Deaktivieren der Kontrollkästchen **Benutzereinstellungen überschreiben** auf ihre Standardwerte zurückgesetzt werden.

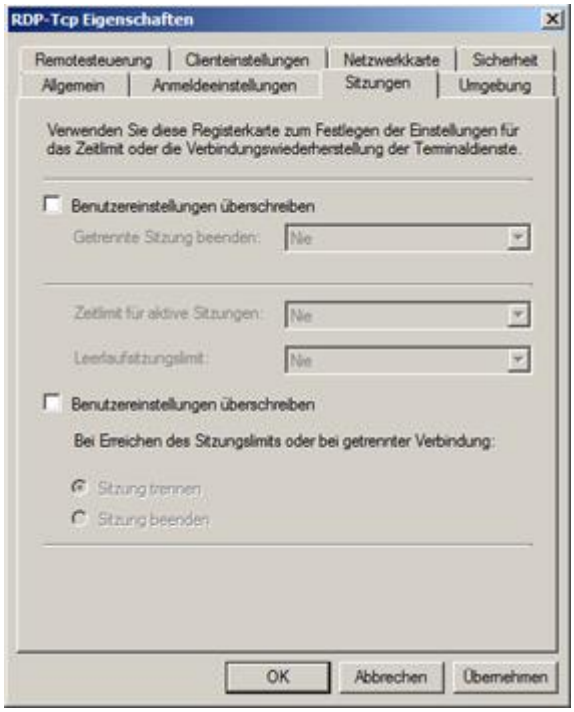

Abbildung 23. Korrekte Einstellungen des Terminal-Servers

Hinweis. Im Betriebssystem Windows Server 2008 R2 werden die Terminal-Dienste als Remote-Desktop-Dienste bezeichnet.

Installation der Software für Remotesteuerung

Wenn Sie Remote-Verbindungen zu ViPNet Netzwerkknoten mit Hilfe von externen Programmen wie Remote Administrator (Radmin), VNC oder Remote Desktop Connection aufbauen möchten, dann stellen Sie zunächst sicher, dass die angegebenen Programme auf Ihrem Computer installiert sind.

Sie erhalten die Installationspakete für diese Programme, indem Sie die Pakete von den folgenden Webseiten herunterladen:

- Remote Administrator: von der Web-Seite Radmin http://www.radmin.com/download/. Das Paket Remote Administrator umfasst Client- und Server-Softwaremodule.
- VNC: von der Web-Seite RealVNC http://www.realvnc.com/download.html. Das Paket VNC umfasst Client- und Server-Softwaremodule.
- Remote Desktop Connection: von der Microsoft Web-Seite http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=80111F21-D48D-426E-96C2-08AA2BD23A49. Das Programm Remote Desktop Connection ist in den Betriebssystemen Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8 standardmäßig installiert. Die Verbindungen können von allen Computern aufgebaut werden, die eine beliebige Version der aufgeführten Betriebssysteme benutzen. Als Zielcomputer können jedoch nur Computer auftreten, auf denen die Betriebssystemversion „Enterprise", „Professional" oder „Ultimate" installiert ist. Ausführliche Informationen sind auf der Webseite von Microsoft enthalten http://windows.microsoft.com/de-de/windows-8/remote-desktop-connection-frequently-asked-questions.

Starten des Programms für die Remotesteuerung

Die Software ViPNet Monitor ermöglicht den Remote-Zugriff auf ViPNet Netzwerkknoten mit Hilfe von externen Programmen wie Remote Administrator (Radmin), VNC oder Remote Desktop Connection. Der Remotezugang kann für den Administrator eines Knotens nützlich sein, falls der physikalische Zugang zu diesem Knoten erschwert ist. Ebenso kann der Remotezugang von einem Benutzer verwendet werden, der von zu Hause aus auf einem Computer im Büro arbeiten möchte.

Zum Starten eines Programms für den Remote-Zugriff:

1. Wählen Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Privates Netzwerk**.
2. Klicken Sie mit der rechten Maustaste auf den Netzwerkknoten, auf den remote zugegriffen werden soll, zeigen Sie im Kontextmenü auf den Eintrag **Externe Programme** und wählen dann den Startbefehl für das benötigte Remotezugriffsprogramm aus.

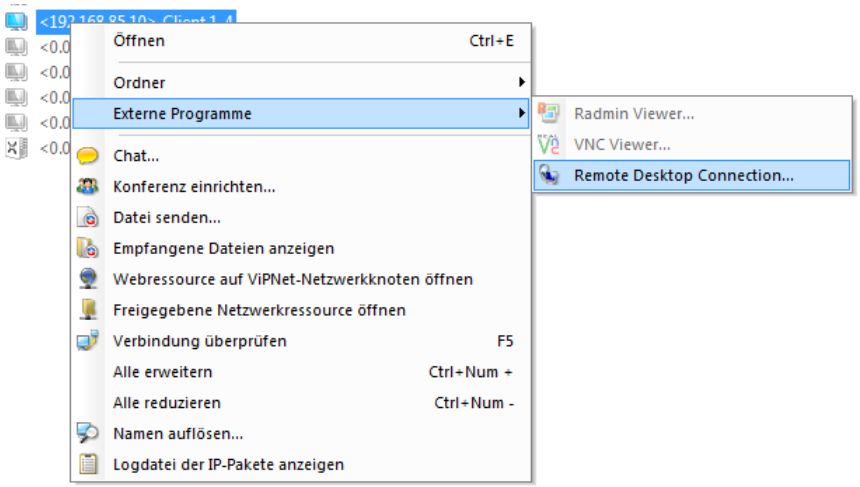

Abbildung 24. Starten einer externen Anwendung

Die Befehle im Untermenü **Externe Programme** sind nur dann aktiv, wenn die entsprechenden Programme auf dem Computer installiert sind (s. Installation der Software für Remotesteuerung auf S. 43). Außerdem sollte der gewählte Netzwerkknoten eine von Null abweichende Zugangs-IP-Adresse besitzen. Zusätzlich sollte auf diesem Knoten die entsprechende Server-Software (z.B. Radmin Server, VNC Server) installiert, konfiguriert und gestartet sein.

Hinweis. Beim Verwenden des Programms Remote Desktop ist es nicht erforderlich, zusätzliche Server-Software auf dem Knoten zu installieren. Mit Hilfe von Remote Desktop kann der Remote-Zugriff zu beliebigen ViPNet Netzwerkknoten aufgebaut werden, die unter dem Betriebssystem Windows arbeiten.

Falls alle genannten Bedingungen erfüllt sind, öffnet sich das Verbindungsfenster. Sobald die Verbindung aufgebaut ist, wird das Eingabefenster für das Zugangspasswort für den gewählten Knoten angezeigt. Nach der Eingabe des Passworts wird ein Fenster geöffnet, das den Desktop des Remoteknotens anzeigt.

Hinweis. Es sollte beachtet werden, dass für einen erfolgreichen Verbindungsaufbau zu einem ViPNet Netzwerkknoten die Software für den Remote-Zugriff korrekt konfiguriert sein sollte.

Bei Verwendung des Programms Remote Desktop sollten zum Beispiel auf dem Netzwerkknoten, zu dem die Verbindung hergestellt wird, die folgenden Einstellungen vorgenommen werden:

- Remote-Verbindungen sollten in den Systemeigenschaften erlaubt sein.
- Das Benutzerkonto des externen Benutzers sollte zur Liste der Remote-Benutzern hinzugefügt werden.

7

Verbindungen zwischen ViPNet VPN- Netzwerk und einem Netzwerk auf Basis der Software ViPNet Administrator

Allgemeine Informationen 47

Initiierung der Verbindung mit Hilfe des ViPNet Network Manager 48

Initiierung der Verbindung mit Hilfe der Software ViPNet Administrator 50

Anforderungen an die Partnernetzwerk-Informationen des ViPNet Netzwerks unter der Steuerung von ViPNet Administrator 52

Allgemeine Informationen

Achtung! In diesem Kapitel wird ausschließlich die Verbindung zwischen einem ViPNet VPN- und einem Netzwerk auf Basis der Software ViPNet Administrator behandelt. Die Verbindung zwischen zwei ViPNet VPN-Netzwerken wird im Dokument „ViPNet VPN. Benutzerhandbuch" behandelt.

ViPNet Administrator stellt eine komplexe Lösung aus Soft- und Hardwarekomponenten dar, die folgende zwei Hauptaufgaben erfüllen soll:

- Einrichtung einer geschützten Umgebung für die sichere Übertragung von vertraulichen Daten unter Verwendung öffentlicher Verbindungskanäle oder Standleitungen (Internet-, Telefonleitungen, u. s. w.) durch Installation eines virtuellen privaten Netzwerks (VPN).
- Aufbau eines Systems öffentlicher Schlüssel (PKI) und Einrichtung einer Zertifizierungsstelle mit dem Ziel, die Verwendung von digitalen Signaturen in den verschiedenen Softwareanwendungen zu ermöglichen.

Es besteht die Möglichkeit, Partnernetzwerk-Verbindungen zwischen einem geschützten Netzwerk auf Basis von ViPNet VPN 4.2 und einem Netzwerk unter der Verwaltung von ViPNet Administrator Version 3.1.2 und höher aufzubauen. In diesem Abschnitt wird das Zusammenwirken des ViPNet VPN-Netzwerks und des Netzwerks unter der Steuerung von ViPNet Administrator 4.2.x beschrieben. Als Initiator der Partnernetzwerk-Verbindung kann dabei sowohl der Administrator des ViPNet VPN-Netzwerks als auch der Administrator des Netzwerks unter der Steuerung von Software ViPNet Administrator auftreten.

Das Netywerk unter der Steuerung von ViPNet Administrator enthält mehr als zehn verschiedenen Software-Komponenten und Modulen, und die Struktur eines ViPNet Netzwerkes unter der Steuerung von Software ViPNet Administrator ist komplexer als die Struktur eines ViPNet VPN-Netzwerks. Deswegen sollte die Verbindung zwischen einem ViPNet VPN- und einem ViPNet Netzwerk unter dem Steuerung von ViPNet Administrator in einer bestimmten Reihenfolge aufgebaut werden (s. Abschnitte unten). Die vom Administrator des Netzwerks unter der Steuerung von ViPNet Administrator übermittelte Partnernetzwerk-Information sollte eine Reihe von Anforderungen erfüllen (s. Anforderungen an die Partnernetzwerk-Informationen des ViPNet Netzwerks unter der Steuerung von ViPNet Administrator auf S. 52).

Es wird empfohlen, die Einrichtung der Partnernetzwerk-Verbindung ausgehend vom ViPNet Administrator nur bei Bedarf zu verwenden.

Achtung! Eine Partnernetzwerk-Verbindung mit einem Netzwerk unter der Steuerung von ViPNet Administrator ist nicht möglich, wenn das Programm ViPNet Network Manager in Ihrem Netzwerk auf einem Coordinator installiert ist.

Initiierung der Verbindung mit Hilfe des ViPNet Network Manager

Als bevorzugte Option zur Einrichtung einer Partnernetzwerk-Verbindung zwischen einem Netzwerk unter der Steuerung von ViPNet Network Manager und einem Netzwerk unter der Steuerung von ViPNet Administrator kann der Ansatz gewählt werden, bei welchem die Verbindung vom Administrator des ViPNet VPN-Netzwerks initiiert wird. In diesem Fall umfasst der Vorgang der Verbindungseinrichtung drei Etappen:

1. Initiierung der Partnernetzwerk-Verbindung durch den Administrator der Software ViPNet Network Manager.
2. Der Empfang und die Verarbeitung der Partnernetzwerk-Informationen durch den Administrator des ViPNet Netzwerks (unter der Steuerung von ViPNet Administrator), die Herstellung von Verbindungen zwischen diesen Netzwerken, der Versand der sogenannten Antwortdatei mit Exportdaten in das Netzwerk unter der Steuerung von ViPNet Network Manager. Die Antwortdatei sollte dabei bestimmte Anforderungen erfüllen (s. Anforderungen an die Partnernetzwerk-Informationen des ViPNet Netzwerks unter der Steuerung von ViPNet Administrator auf S. 52).
3. Empfang von Exportdateien im ViPNet Network Manager, Bestätigung der Verbindungen mit den Knoten anderes Netzwerks, Fertigstellung der etablierten Partnernetzwerk-Verbindung.

Zum Einrichten einer Partnernetzwerk-Verbindung sollten die folgenden Schritte durchgeführt werden:

1. Erstellen Sie im ViPNet Network Manager zum Initiieren der Partnernetzwerk-Verbindung eine Datei mit den Partnernetzwerk-Informationen. Diese Datei sollte durch ein Passwort geschützt sein und folgende Elemente enthalten: Name und Nummer des Partnernetzwerks unter der Steuerung von ViPNet Administrator, Gateway-Coordinator, Liste der ViPNet VPN-Netzwerkknoten, die an der Partnernetzwerk-Verbindung teilnehmen sollen.

   Leiten Sie die Datei mit den Partnernetzwerk-Informationen und das Passwort auf eine sichere Art an den Administrator des Netzwerks unter der Steuerung von ViPNet Administrator weiter.
2. Der Administrator anderes Netzwerks sollte folgendermaßen in der Software ViPNet Administrator vorgehen, um die Partnernetzwerk-Informationen zu verarbeiten:
   - Die Partnernetzwerk-Informationen in Form eines Archivs im `*.lzh`-Format empfangen.
   - Im Programm ViPNet Network Control Center:
     - Die Datei mit den Partnernetzwerk-Informationen im Fenster der Partnernetzwerke annehmen.
     - Den Namen des ViPNet VPN-Partnernetzwerks und den Gateway-Coordinator angeben, die Einrichtung des Partnernetzwerks bestätigen.
   - Die `*.lzh`-Datei in einen separaten Ordner entpacken.
   - Im Programm ViPNet Key and Certification Authority:
     - Im Schlüsselcenter den Internetzwerk-Masterschlüssel mit der Erweiterung `*.key` unter Verwendung des Schutzpassworts, das im Programm ViPNet Network Manager definiert wurde, aus dem Ordner laden.

- Den Internetzwerk-Masterschlüssel aktivieren und als aktuellen Schlüssel festlegen.

- Im Programm ViPNet Network Control Center:
  - Im Fenster der Partnernetzwerke die Benutzer des Netzwerks unter der Steuerung von ViPNet Administrator auswählen, die an den Partnernetzwerk-Verbindungen teilnehmen sollen.
  - Die Verbindungen zwischen den Benutzern eigenes Netzwerks und den Benutzern des Netzwerks unter der Steuerung von ViPNet Administrator definieren.
  - Ausgehende Partnernetzwerk-Informationen für das ViPNet VPN-Netzwerk zusammenstellen und in ein `*.lzh`-Archiv verpacken.
- Die erstellten Exportdateien mit den Partnernetzwerk-Informationen in Form eines `*.lzh`-Archivs an den Administrator des ViPNet Network Manager weiterleiten.

3 Empfangen Sie die Partnernetzwerk-Informationen aud dem Netzwerk unter der Steuerung von ViPNet Administrator und gehen dann folgendermaßen vor:

- Nehmen Sie im Programm ViPNet Network Manager die eingehenden Partnernetzwerk-Informationen aus anderem Netzwerk, indem Sie den Pfad zum erhaltenen `*.lzh`-Archiv angeben.

  Der Assistent für Partnernetzwerk-Verbindungen überprüft, ob die erhaltene Datei mit dem ViPNet Network Manager kompatibel ist. Wenn die erhaltenen Partnernetzwerk-Informationen inkorrekte Daten enthalten, können die Informationen nicht bearbeitet werden. Auf der Seite des Assistenten wird eine entsprechende Fehlermeldung angezeigt (s. Abbildung 25 auf S. 49) und ein Fehlbericht wird erstellt. In diesem Fall sollten Sie den Fehlerbericht an den Administrator des ViPNet Netzwerks auf Basis der Software ViPNet Administrator überreichen, damit die Partnernetzwerk-Informationen korrigiert und erneut versendet werden können.

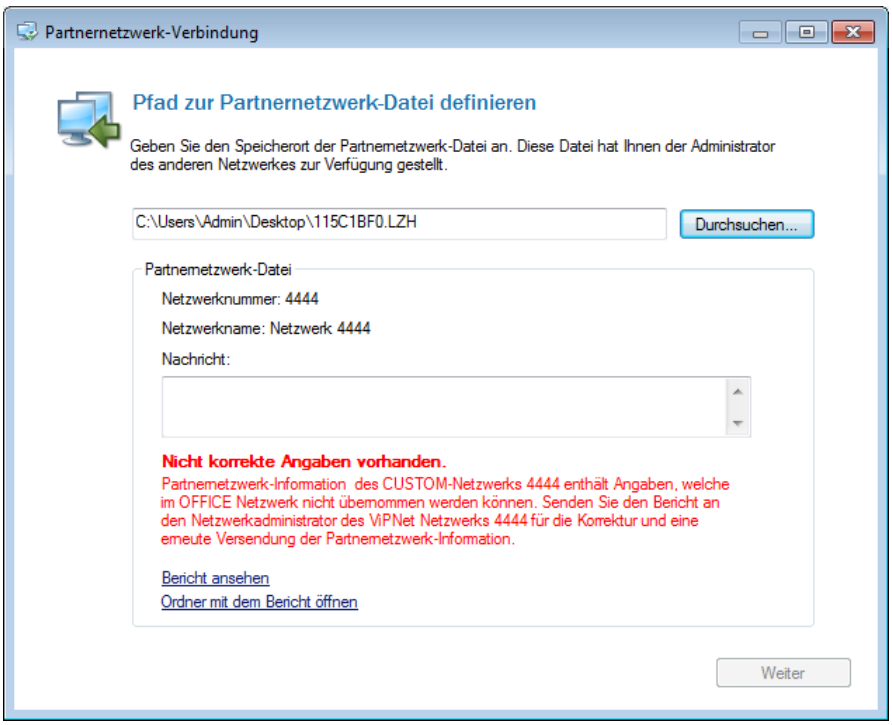
Partnernetzwerk-Verbindung
Pfad zur Partnernetzwerk-Datei definieren
Geben Sie den Speicherort der Partnernetzwerk-Datei an. Diese Datei hat Ihnen der Administrator des anderen Netzwerkes zur Verfügung gestellt.
C:\Users\Admin\Desktop\115C1BF0.LZH
Durchsuchen...
Partnernetzwerk-Datei
Netzwerknummer: 4444
Netzwerkname: Netzwerk 4444
Nachricht:
Nicht korrekte Angaben vorhanden.
Partnernetzwerk-Information des CUSTOM-Netzwerks 4444 enthält Angaben, welche im OFFICE Netzwerk nicht übernommen werden können. Senden Sie den Bericht an den Netzwerkadministrator des ViPNet Netzwerks 4444 für die Korrektur und eine erneute Versendung der Partnernetzwerk-Information.
Bericht ansehen
Ordner mit dem Bericht öffnen
Weiter

Abbildung 25. Partnernetzerk-Information enthält inkorrekte Daten

Wenn die erhaltenen Partnernetzwerk-Informationen Daten enthalten, die möglicherweise zu Konfliktsituationen führen können, dann werden diese Daten nicht übernommen. Im Assistentenfenster wird eine Meldung über mögliche Konflikte angezeigt (s. Abbildung 26 auf S. 50).

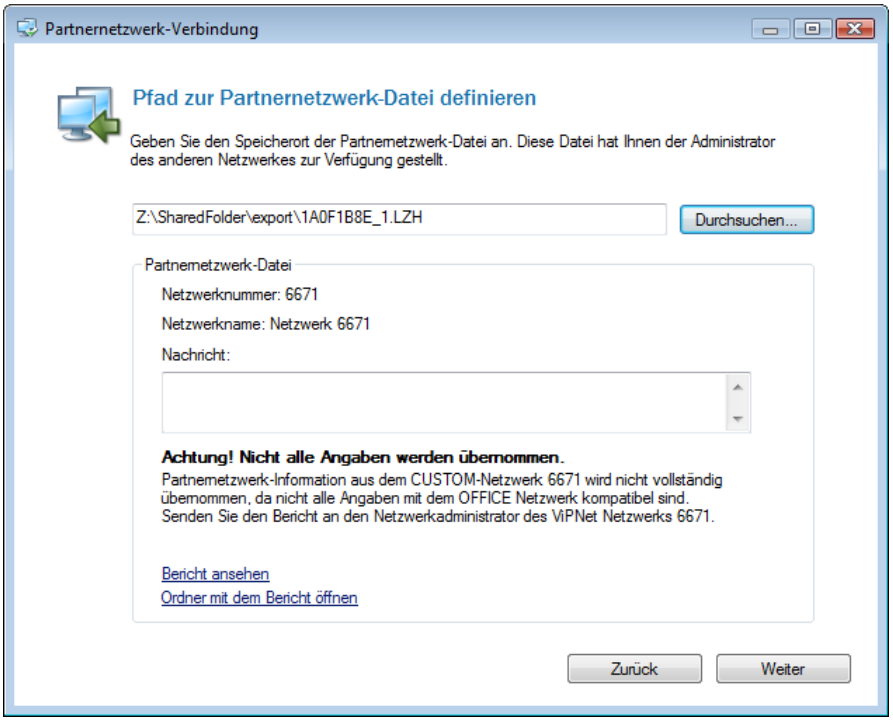
Partnernetzwerk-Verbindung
Pfad zur Partnernetzwerk-Datei definieren
Geben Sie den Speicherort der Partnernetzwerk-Datei an. Diese Datei hat Ihnen der Administrator des anderen Netzwerkes zur Verfügung gestellt.
Z:\SharedFolder\export\1A0F1B8E_1.LZH
Durchsuchen...
Partnernetzwerk-Datei
Netzwerknummer: 6671
Netzwerkname: Netzwerk 6671
Nachricht:
Achtung! Nicht alle Angaben werden übernommen.
Partnernetzwerk-Information aus dem CUSTOM-Netzwerk 6671 wird nicht vollständig übernommen, da nicht alle Angaben mit dem OFFICE Netzwerk kompatibel sind.
Senden Sie den Bericht an den Netzwerkadministrator des ViPNet Netzwerks 6671.
Bericht ansehen
Ordner mit dem Bericht öffnen
Zurück
Weiter

Abbildung 26. Angaben werden teilweise übernommen

- Bestätigen Sie die Verbindungen zu den Knoten des Partnernetzwerks.
- Erstellen und versenden Sie die aktualisierten Schlüssel für Ihres Netzwerk.
- Sicherstellen, dass alle Updates übernommen wurden und die Partnernetzwerk-Verbindung eingerichtet ist.

Initiierung der Verbindung mit Hilfe der Software ViPNet Administrator

Hinweis. In diesem Abschnitt wird die Arbeit mit den Programmen ViPNet Administrator der Version 4.2.x beschrieben.

Die Vorgehensweise zur Einrichtung einer Partnernetzwerk-Verbindung, bei welcher die Verbindung mit Hilfe der Software ViPNet Administrator initiiert wird, stellt nicht die bevorzugte Variante dar und sollte daher nur bei Bedarf verwendet werden. In diesem Fall umfasst der Vorgang der Verbindungseinrichtung drei Etappen:

1. Initiierung der Partnernetzwerk-Verbindung durch das Netzwerk unter der Steuerung von ViPNet Administrator. Der primäre Export sollte dabei bestimmte Anforderungen erfüllen (s. Anforderungen an die Partnernetzwerk-Informationen des ViPNet Netzwerks unter der Steuerung von ViPNet Administrator auf S. 52).
2. Empfang und Verarbeitung von Partnernetzwerk-Informationen durch ViPNet Network Manager, Versand einer Antwortdatei mit Exportdaten an das ViPNet Netzwerk unter der Steuerung von ViPNet Administrator.
3. Empfang der Exportdatei mit Hilfe der Software ViPNet Administrator, Bestätigung der Verbindungen zwischen den Netzwerkknoten dieser Netzwerke, Fertigstellen der Einrichtung der Partnernetzwerk-Verbindung.

Zum Einrichten einer Partnernetzwerk-Verbindung sollten die folgenden Schritte durchgeführt werden:

1. Die Partnernetzwerk-Verbindung wird in einem Netzwerk unter der Steuerung von ViPNet Administrator initiiert. Es sollten dabei primäre Exportdaten auf die folgende Weise generiert werden:
   - Wählen Sie im Programm ViPNet Network Control Center die Benutzer des Netzwerks aus, die an der Partnernetzwerk-Verbindung teilnehmen sollen.
   - Erstellen Sie die primäre Exportdatei (Archiv *.lzh).
   - Generieren Sie im Programm ViPNet Zertifizierungsstelle einen Internetzwerk-Masterschlüssel, exportieren diesen in eine Datei und legen ihn als aktuellen Schlüssel fest.
   - Entpacken Sie das Archiv `*.lzh` und kopieren den Namen der Datei mit der Erweiterung `*.vpn`.
   - Wechseln Sie in den Ordner mit dem exportierten Internetzwerk-Masterschlüssel. Benennen Sie den Schlüssel in Übereinstimmung mit dem Namen der Datei `*.vpn` aus dem Archiv `*.lzh` um (die Erweiterung der Datei des Internetzwerk-Masterschlüssels sollte dabei nicht geändert werden).
   - Fügen Sie die Datei mit dem exportierten Masterschlüssel zum Archiv `*.lzh` hinzu und verpacken Sie das Archiv.
   - Leiten Sie die exportierten Internetzwerk-Informationen in Form des Archivs `*.lzh` an den Administrator des ViPNet VPN-Netzwerks weiter.
2. Übernehmen Sie die aus der Software ViPNet Administrator übermittelten Partnernetzwerk-Informationen und führen Sie dann die folgenden Schritte aus:
   - Nehmen Sie im Programm ViPNet Network Manager die eingehenden Partnernetzwerk-Informationen aus anderem Netzwerk, indem Sie den Pfad zum erhaltenen `*.lzh`-Archiv angeben.

     Der Assistent für Partnernetzwerk-Verbindungen überprüft, ob die erhaltene Datei mit dem ViPNet Network Manager kompatibel ist. Wenn die erhaltenen Partnernetzwerk-Informationen inkorrekte Daten enthalten, können die Informationen nicht bearbeitet werden. Auf der Seite

des Assistenten wird eine entsprechende Fehlermeldung angezeigt (s. Abbildung 25 auf S. 49) und ein Fehlbericht wird erstellt. In diesem Fall sollten Sie den Fehlerbericht an den Administrator des ViPNet Netzwerks auf Basis der Software ViPNet Administrator überreichen, damit die Partnernetzwerk-Informationen korrigiert und erneut versendet werden können.

Wenn die erhaltenen Partnernetzwerk-Informationen Daten enthalten, die möglicherweise zu Konfliktsituationen führen können, dann werden diese Daten nicht übernommen. Im Assistentenfenster wird eine Meldung über mögliche Konflikte angezeigt (s. Abbildung 26 auf S. 50).

- Definieren Sie die Verbindungen zwischen den Knoten Ihres Netzwerks und des Netzwerks unter der Steuerung von ViPNet Administrator.
- Generieren Sie Schlüsseldistributionen der geänderten Schlüssel für Ihre Netzwerk.
- Speichern Sie die ausgehende Partnernetzwerk-Informationen für das Netzwerk unter der Steuerung von ViPNet Administrator in einer Datei ab.
- Leiten Sie die generierte Exportdatei mit Internetzwerk-Informationen in Form des Archivs `*.lzh` an das Netzwerk unter der Steuerung von ViPNet Administrator weiter.

3 In dem Netzwerk unter der Steuerung von ViPNet Administrator sollte Folgendes durhcgeführt werden:

- Im Programm ViPNet Network Control Center:
  - Die erhaltene Datei mit den Partnernetzwerk-Informationen im Fenster der Partnernetzwerke laden.
  - Die neu erstellten Verbindungen beim Laden der Informationen bestätigen.
  - Adresslisten und Schlüssel für die gesamte Liste der Netzwerkknoten erstellen.
- Im Programm ViPNet Key and Certificate Authority:
  - Schlüsselupdates für die Netzwerkknoten des eigenen Netzwerks im Schlüsselcenter erstellen.
  - Die erstellten Updates an das Programm ViPNet Network Control Center weiterleiten.
  - Die Adresslisten und Schlüssel im Programm ViPNet Network Control Center an allen Knoten versenden.
- Sicherstellen, dass alle Updates übernommen wurden und die Partnernetzwerk-Verbindung eingerichtet ist.

Anforderungen an die Partnernetzwerk-Informationen des ViPNet Netzwerks unter der Steuerung von ViPNet Administrator

Die Software ViPNet Administrator vereinigt die VPN-Technologie und die PKI-Mechanismen, wodurch viele unterschiedliche Szenarien zum Schutz von Daten in modernen Netzwerken verwirklicht werden

können. ViPNet Netzwerke unter Steuerung von ViPNet Administrator verfügen über eine komplexe Struktur. Einige Objekte und Begriffe, die in ViPNet Netzwerken unter der Steuerung von ViPNet Administrator verwendet werden, finden keine Entsprechung in ViPNet VPN-Netzwerken. Dadurch können Partnernetzwerk-Informationen aus einem ViPNet Netzwerk unter der Steuerung von ViPNet Administrator die Daten enthalten, die Konfliktsituationen verursachen können.

Bei der Bearbeitung der Partnernetzwerk-Informationen aus dem ViPNet Netzwerk unter der STeuerung von ViPNet Administrator überprüft der Assistent für Partnernetzwerk-Verbindungen, ob alle Angaben für das ViPNet VPN-Netzwerk zulässig sind und dort verwendet werden können. Wenn unzulässige Angaben festgestellt werden, wird die Bearbeitung der Partnernetzwerk-Informationen abgebrochen, eine entsprechende Meldung angezeigt und ein Fehlerbericht erstellt. In diesem Fall sollte der Bericht über unzulässige Angaben in den Partnernetzwerk-Informationen an den Administrator des ViPNet Netzwerks unter der Steuerung von ViPNet Administrator übermittelt werden, damit die Partnernetzwerk-Informationen korrigiert und erneut versendet werden können.

Der Assistent für Partnernetzwerk-Verbindungen führt die Verarbeitung von Partnernetzwerk-Informationen aus dem ViPNet Netzwerk unter der Steuerung von ViPNet Administrator nicht durch, wenn folgende Begebenheiten festgestellt werden:

- Eingehende Partnernetzwerk-Informationen aus dem Netzwerk unter der Steuerung von ViPNet Administrator enthalten keinen einzigen Netzwerkknoten, der in der Rolle „Network Control Center" registriert ist.
- Eingehende Partnernetzwerk-Informationen enthalten keine Daten über den Gateway-Coordinator.
- Auf dem Netzwerkknoten, der in der Rolle „Network Control Center" registriert ist oder als Gateway-Coordinator auftritt, ist ein Benutzer registriert, der bereits auf anderen Netzwerkknoten registriert ist (in diesem Fall werden Informationen über den Netzwerkknoten nicht geladen).
- Auf dem Netzwerkknoten, der in der Rolle „Network Control Center" registriert ist oder als Gateway-Coordinator auftritt, ist kein einziger Benutzer registriert (in diesem Fall werden Informationen über den Netzwerkknoten nicht geladen).

Die Partnernetzwerk-Informationen aus dem ViPNet Netzwerk unter der Steuerung von ViPNet Administrator können Angaben enthalten, die den Aufbau von Partnernetzwerk-Verbindungen ermöglichen, aber gleichzeitig zu Konfliktsituationen führen können. Solche Angaben werden vom Assistenten für Partnernetzwerk-Verbindungen während der Bearbeitung von Daten aus dem Netzwerk unter der Steuerung von ViPNet Administrator nicht übernommen. Dabei wird eine entsprechende Meldung angezeigt und ein Fehlerbericht erstellt.

Die folgenden Angaben werden vom Assistenten nicht übernommen:

- Angaben zu Netzwerkgruppen.
- Informationen über Benutzer, die in einer Netzwerkgruppe registriert sind.
- Informationen über Benutzer, die auf mehr als einem Netzwerkknoten registriert sind.
- Netzwerkknoten, auf denen Benutzer registriert sind, der bereits auf anderen Netzwerkknoten registriert wurden.
- Informationen über Benutzer, die auf keinem einzigen Netzwerkknoten registriert sind.
- Netzwerkknoten, auf denen kein einziger Benutzer registriert ist.

- Daten über Benutzer, die in keiner einzigen Benutzergruppe registriert sind.
- Benutzergruppen, in denen kein einziger Benutzer registriert ist.
- Verbindungen, die Benutzer oder Benutzergruppen enthalten, deren Daten nicht übernommen wurden.

A

Index

A

Automatische Anmeldung in Windows • 36

D

Das Programm ViPNet Network Manager übertragen • 9

I

Installation eines Remotedruckers • 12

P

Partnernetzwerkverbindung • 46
Passwort des ViPNet-Benutzers speichern • 39

R

Remote-Steuerung von ViPNet-Netzwerkknoten • 35
    Installation der Software für Remotesteuerung • 43
    Konfiguration des Terminalservers bei Remotesteuerung • 41

T

Terminalserver • 41
Tunnelung von Knoten, die sich nicht im Subnetz des tunnelnden Coordinators befinden • 16

V

ViPNet Netzwerk auf Basis der Software ViPNet Administrator • 46, 47, 48, 52